

Πανεπιστήμιο Δυτικής Αττικής Τμ. Μηχ/κων Βιομηχανικής Σχεδίασης και Παραγωγής

Σχεδίαση διαδικτυακών εφαρμογών

**Διάλεξη 5: τα διαδικτυακά
πρωτόκολλα**

1-1. Εισαγωγή

Το Διαδίκτυο ξεκίνησε με τη δημιουργία λογισμικού (που αργότερα εξελίχθηκε στο TCP/IP) το οποίο τοποθετούμενο σε υπολογιστές (ξενιστές) τους επέτρεπε να επικοινωνούν μεταξύ τους

- πάνω από διαφορετικά φυσικά δίκτυα
- μέσα από διαφορετικά λειτουργικά συστήματα

Πρώτες εφαρμογές:

- Ηλεκτρονικό ταχυδρομείο (e-mail)
- Μεταφορά αρχείων (ftp)
- Απομακρυσμένη χρήση υπολογιστών (rlogin)

1-2. Ιστορικά στοιχεία

- 1969: Ξεκινά το ARPANET με 4 κόμβους (DARPA)
 - 1973: Ο Vint Cerf Bob και Cahn δημοσιεύουν το TCP
 - 1975: Δημοσιεύεται το e-mail specification (RFC 733)
 - 1983: Το TCP/IP Υιοθετείται ως πρότυπο στο ARPANET
- Επίσης πρώτη σύνδεση της Ελλάδας
- 1984: Εισαγωγή του DNS. 1000 (hosts) ξενιστές
 - 1985: Δημιουργείται το NSFNET στα 56kbps
 - 1988: Αναβαθμίζεται στα 1.544Mbps (T1)
 - 1990: Ο κορμός του NSFNET εκτοπίζει το ARPANET
- Η Ελλάδα μπαίνει στο NSFNET
- 1997: Το Διαδίκτυο φθάνει τα 16 εκ. Hosts, 60 εκ. χρήστες
 - 2004: Πλησιάζει 1 δισ χρήστες.

1-3. Αρχές Λειτουργίας

Προώθηση δεδομενογραμμάτων (με πλήρεις διευθύνσεις)

Δύο βασικά πρωτόκολλα

Στρώμα δικτύου:

- IP: Best-effort service, hop-by-hop routing, άνευ συνδέσεων, ανεξαρτησία από φυσικά δίκτυα

Στρώμα ξενιστή (host-host):

- TCP: Αξιόπιστη μεταφορά αδόμητων bytes με νοητές συνδέσεις και αναμεταδόσεις απωλεσθέντων

4 στρώματα (πρβλ 7 στο OSI)

- Διευθύνσεις IP: 4 byte μήκος, (net id και host id) διακρίνονται σε 4 κλάσεις

2-1. Στοιίβα πρωτοκόλλων

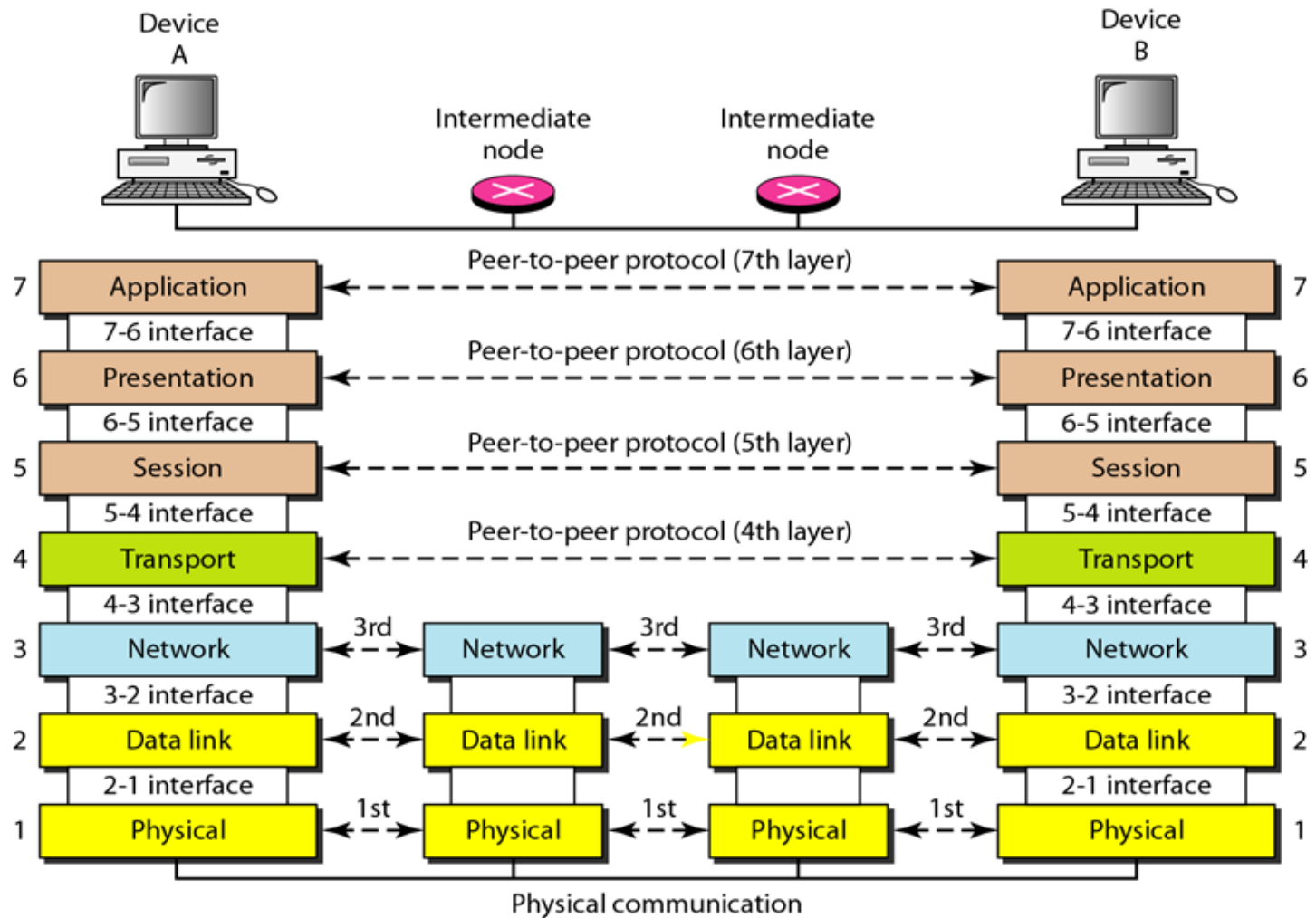
OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	Process
Presentation (6) Formalizes the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Routers IP/IPX/ICMP
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub Land Based Layers	

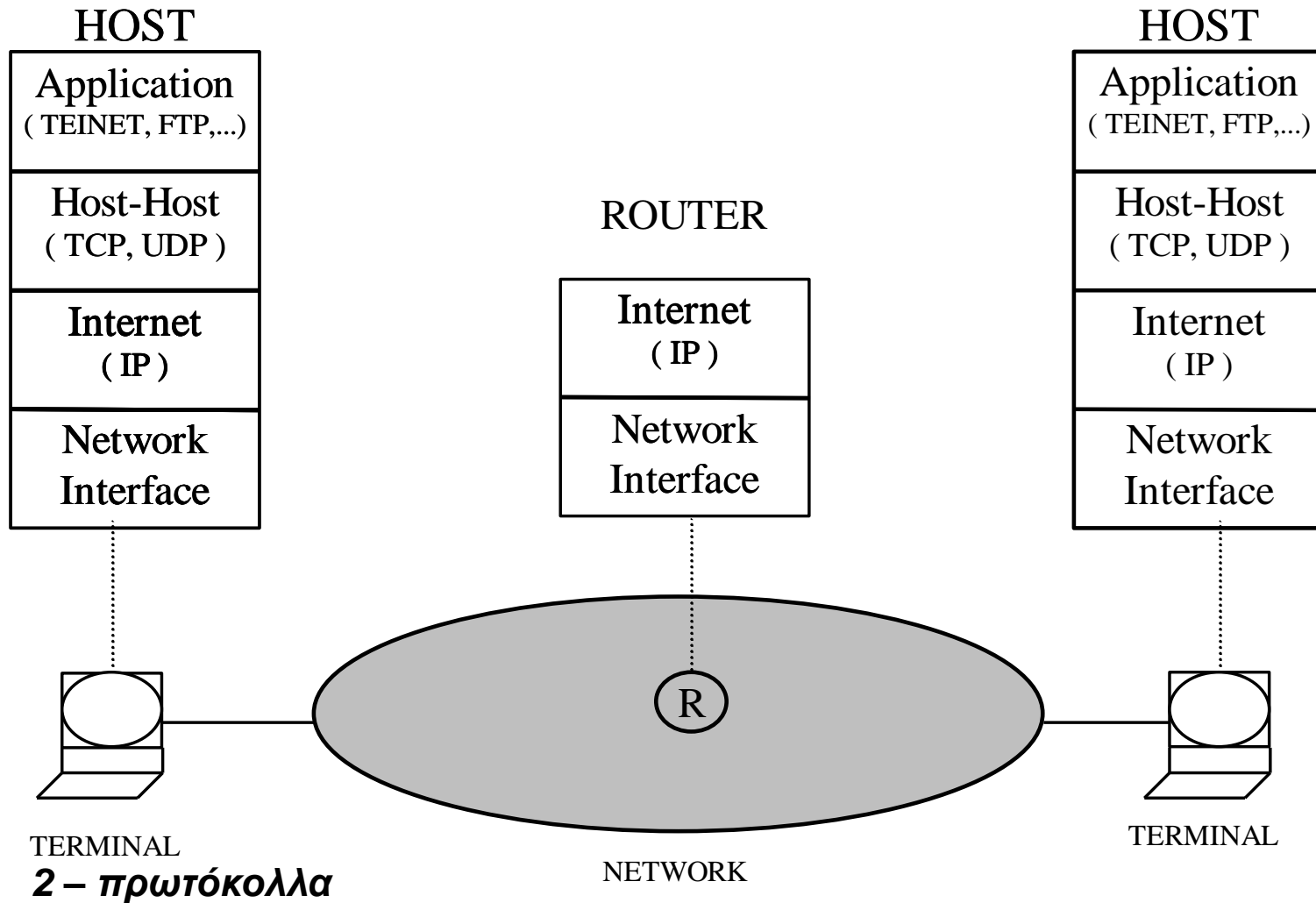
2-1. Στοίβα πρωτοκόλλων

OSI LAYERS	EXAMPLE PROTOCOLS
APPLICATION LAYER	HTTP, FTP, IRC, SSH, DNS
PRESENTATION LAYER	SSL, FTP, IMAP, SSH
SESSION LAYER	VARIOUS API'S, SOCKETS
TRANSPORT LAYER	TCP, UDP, ECN, SCTP, DCCP
NETWORK LAYER	IP, IPSec, ICMP, IGMP
DATA-LINK LAYER	Ethernet, SLIP, PPP, FDDI
PHYSICAL LAYER	Coax, Fiber, Wireless

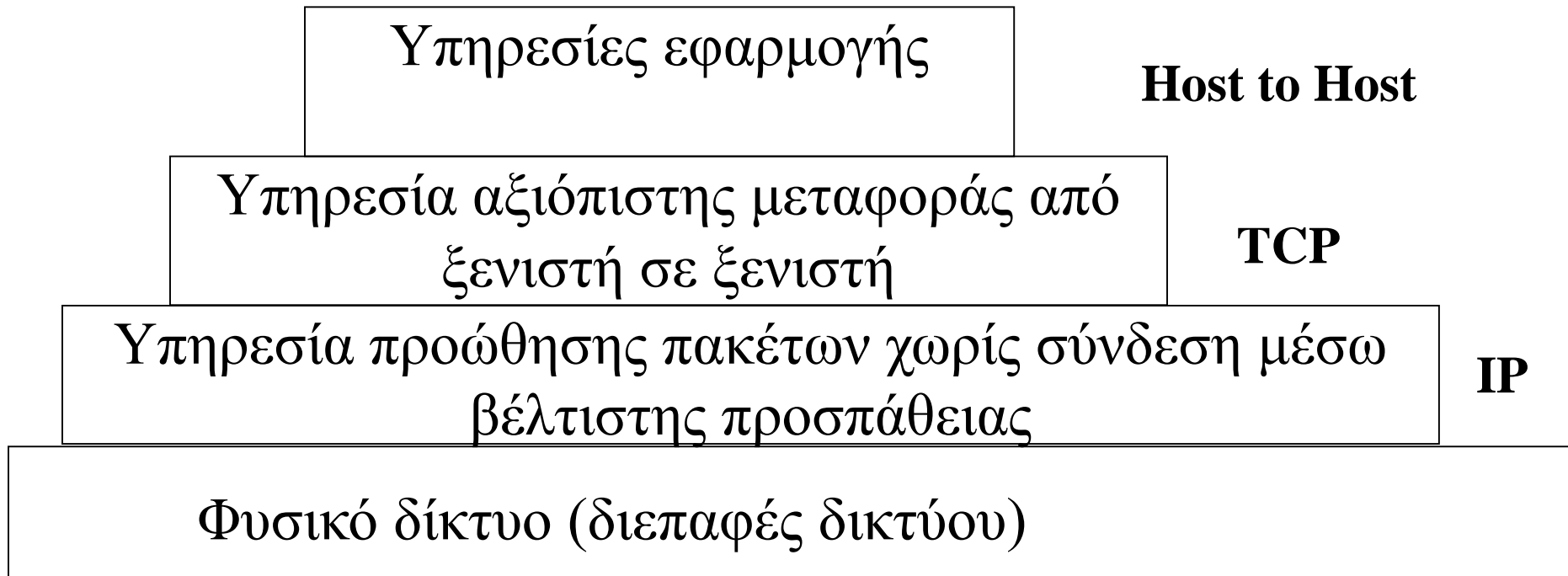
2-1. Στοίβα πρωτοκόλλων



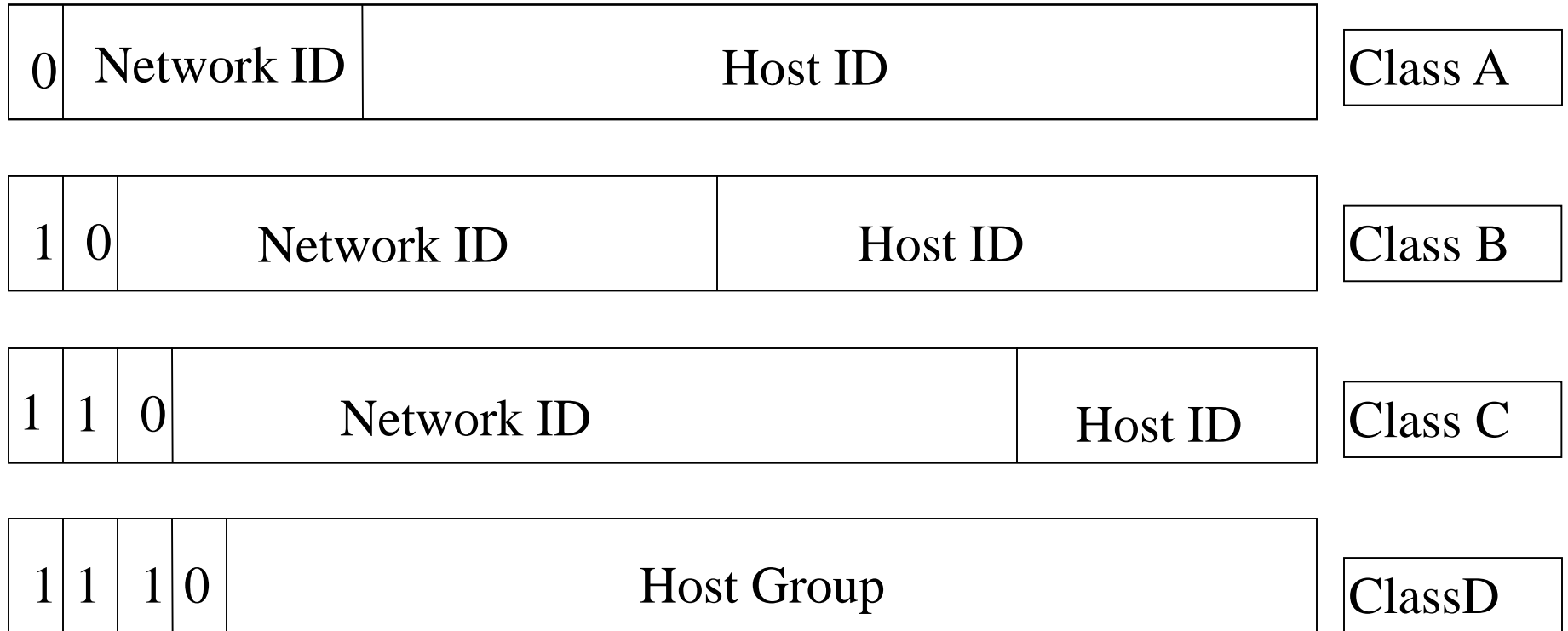
2-1. Στοιβά πρωτοκόλλων



2-2. Τα 4 στρώματα



2-3. Η Φόρμα Διευθύνσεων IP



2-3. Οι διευθύνσεις του Διαδικτύου

- Μια IP address ορίζει μοναδικά μια δικτυακή διεπαφή (κάρτα δικτύου) σε όλο το διαδίκτυο.
- Εξαιρέσεις:
 - Δίκτυα δυναμικής απόδοσης IP (→ DHCP, Lab 7)
 - IP σε private networks (→ NAT, Lab 7)
- Μια IP address:
 - είναι μήκους **32 bit**
 - εμπεριέχει δύο στοιχεία: **network number** και **host number**

2-3. Οι διευθύνσεις του Διαδικτύου

- Το network prefix ορίζει το network και το host number τον συγκεκριμένο host (actually, interface on the network).

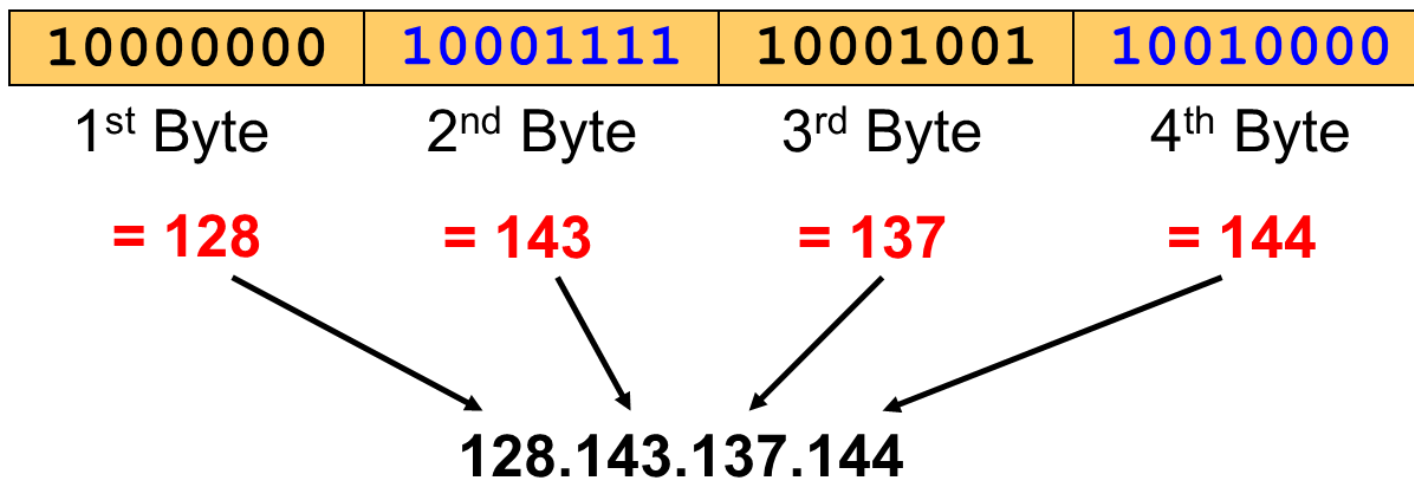
network prefix

host number

- **Πως διαβάζεται μια IP ?**
 - **Before 1993: class-based addressing**
 - or
 - **After 1993: netmask.**

2-3. Οι διευθύνσεις του Διαδικτύου

- Οι IP διευθύνσεις γράφονται με μορφή δεκαδικών αριθμών. (*dotted decimal notation*)
- Κάθε byte παίρνει τιμές στο πεδίο [0..255]:
- **Example:**



2-3. Οι διευθύνσεις του Διαδικτύου

- **Παράδειγμα:** ellington.cs.virginia.edu

128.143

137.144

- Network address : 128.143.0.0 (or 128.143)
- Host number : 137.144
- Netmask: 255.255.0.0 (or ffff0000)
- Prefix or CIDR notation: **128.143.137.144/16**
 - » Network prefix is 16 bits long

2-3. Οι διευθύνσεις του Διαδικτύου

- **special addresses:**

- Loopback interfaces**

- Όλες οι διευθύνσεις 127.0.0.1-127.255.255.255 είναι δεσμευμένες για loopback interfaces
 - Τα περισσότερα συστήματα χρησιμοποιούν την 127.0.0.1
 - Η loopback είναι συσχετισμένη με το λεκτικό “localhost”

- Network address**

- Το host number είναι 0 , π.χ., 128.143.**0.0**

- Broadcast address**

- Host number είναι 1, e.g., 128.143.**255.255**
 - Συχνά αγνοείται για λόγους ασφαλείας.

- **Test / Experimental addresses** (see RFC 1918)

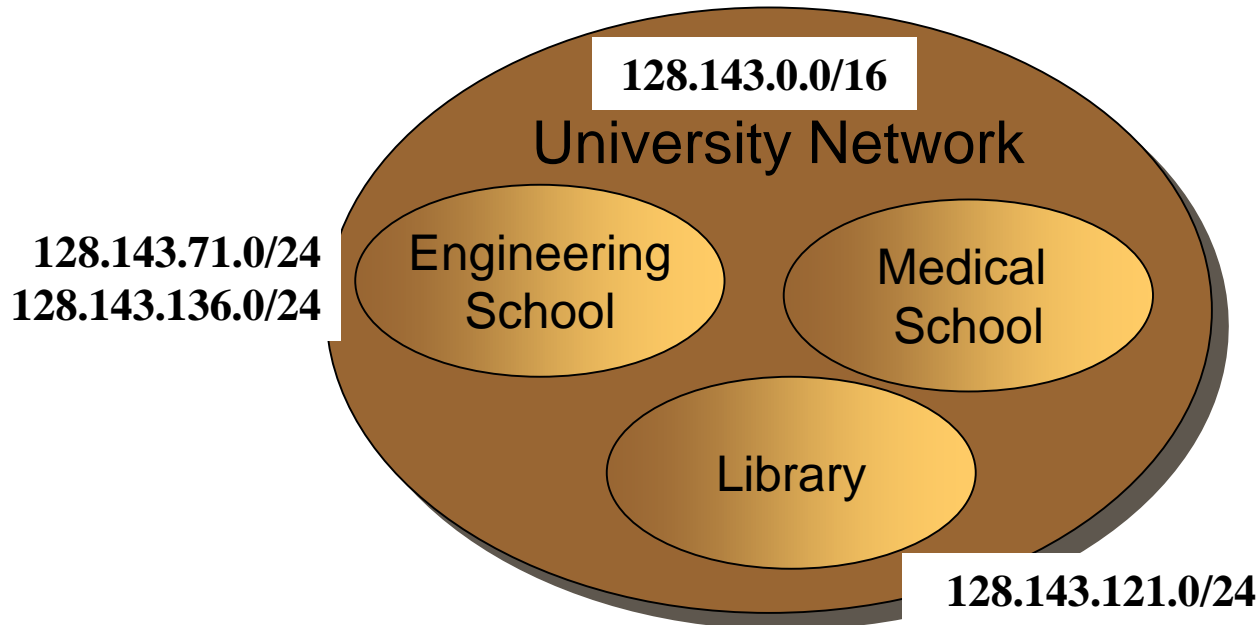
10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

- **Convention (but not a reserved address)**

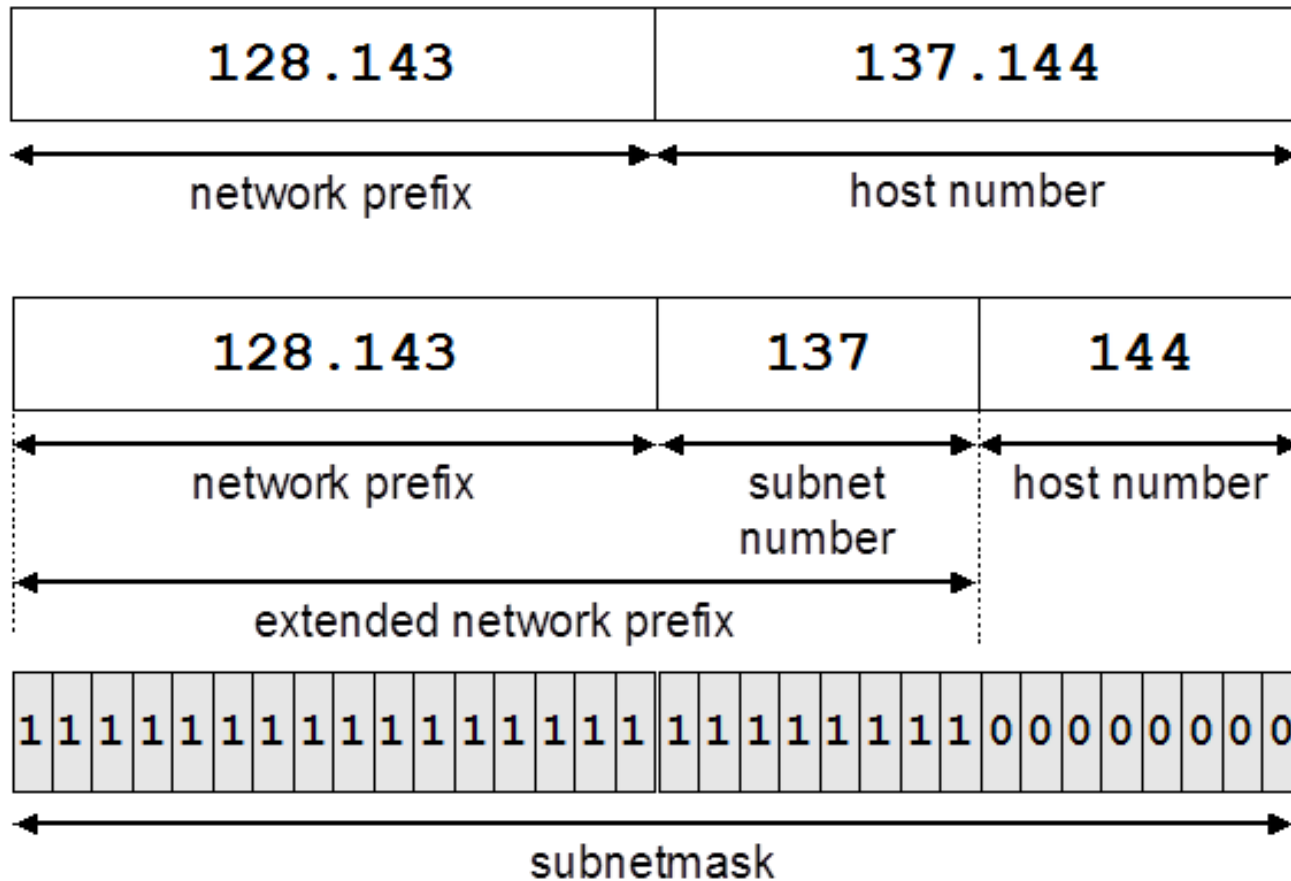
- Default gateway έχει host number ‘1’, e.g., e.g., 192.0.1.1

2-3. Οι διευθύνσεις του Διαδικτύου

- Κάθε τμήμα ενός οργανισμού εξυπηρετείται από ένα εύρος IP διευθύνσεων (subnets or subnetworks)
- Οι διευθύνσεις αυτές πρέπει να είναι διαχωρίσιμες τοπικά.

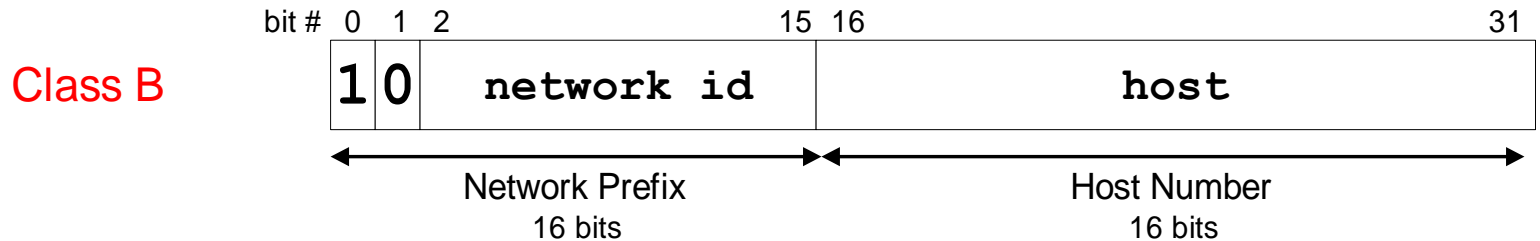
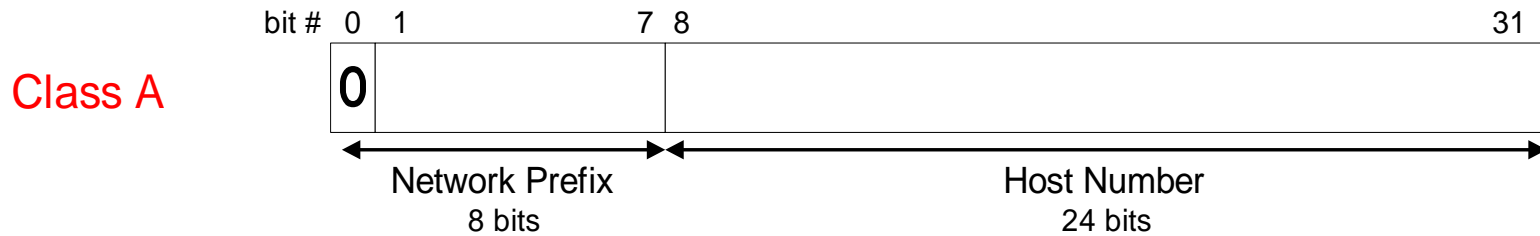


2-3. Οι διευθύνσεις του Διαδικτύου



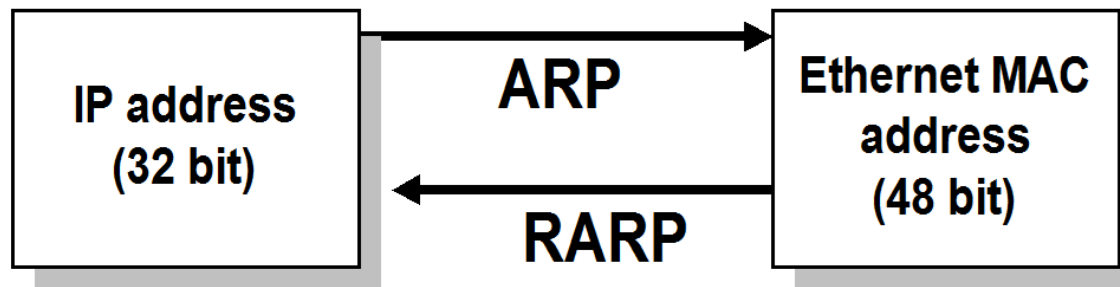
2-3. Οι διευθύνσεις του Διαδικτύου

Οι διευθύνσεις ορισμένες σε κλάσεις (1993):

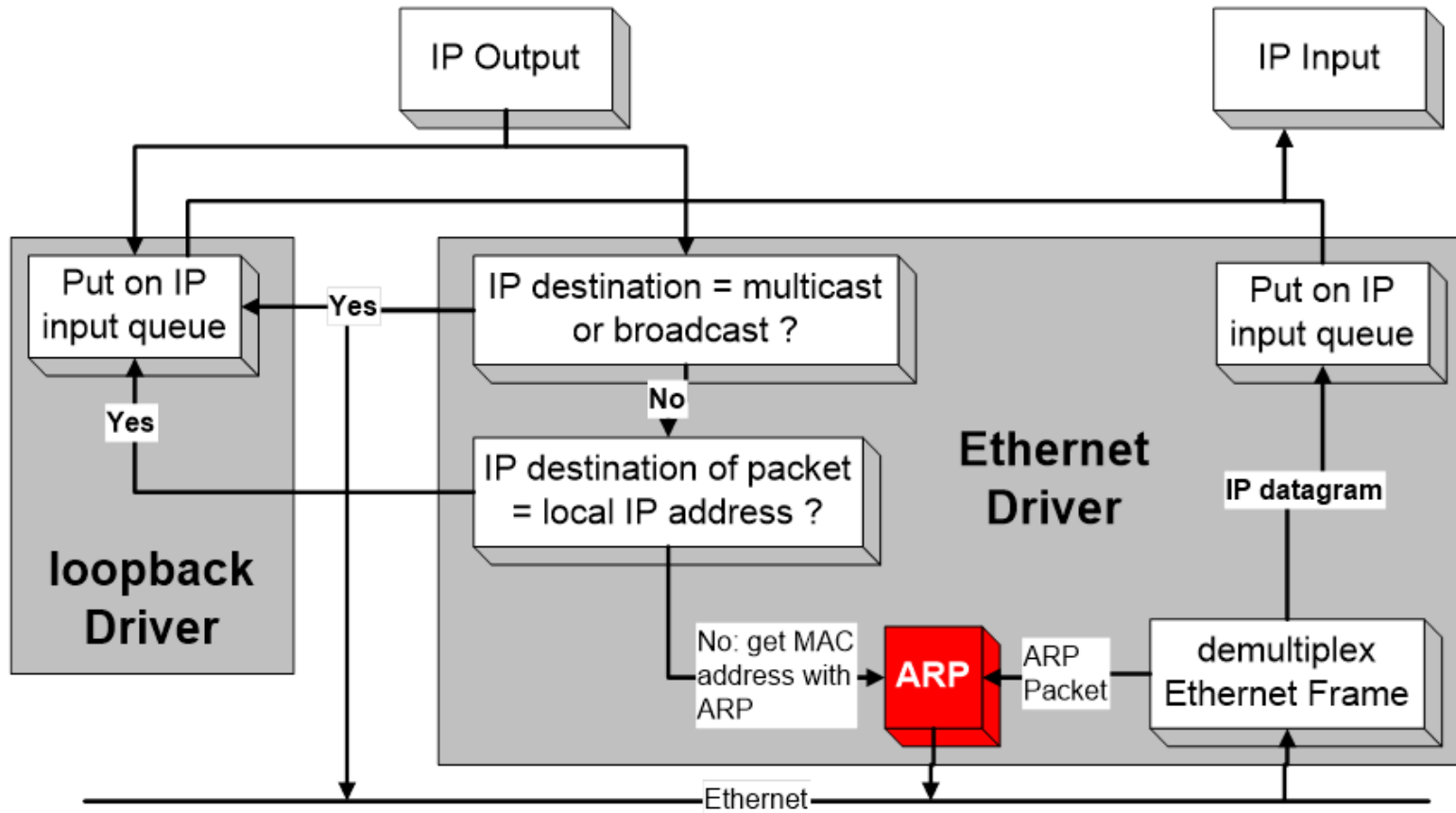


2-4. Φυσικές διευθύνσεις (ARP)

- Note:
 - Το Διαδίκτυο βασίζεται στις IP addresses
 - Τα Data link πρωτόκολλα (Ethernet, FDDI, ATM) μπορεί να έχουν διαφορετικές (MAC) διευθύνσεις.
- Τα ARP and RARP πρωτόκολλα προσφέρουν την αντιστοίχιση των IP διευθύνσεων με MAC
- Ethernet LANs



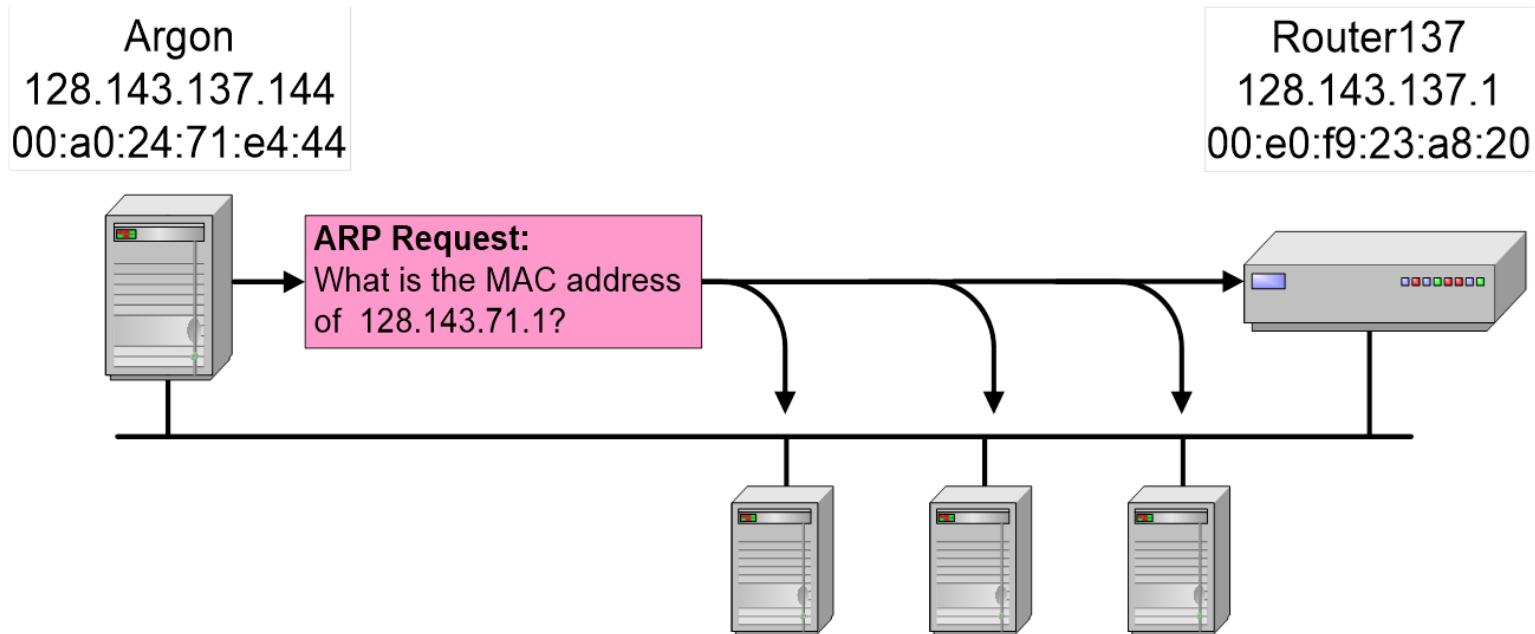
2-4. Φυσικές διευθύνσεις (ARP)



2-4. Φυσικές διευθύνσεις (ARP)

ARP Request:

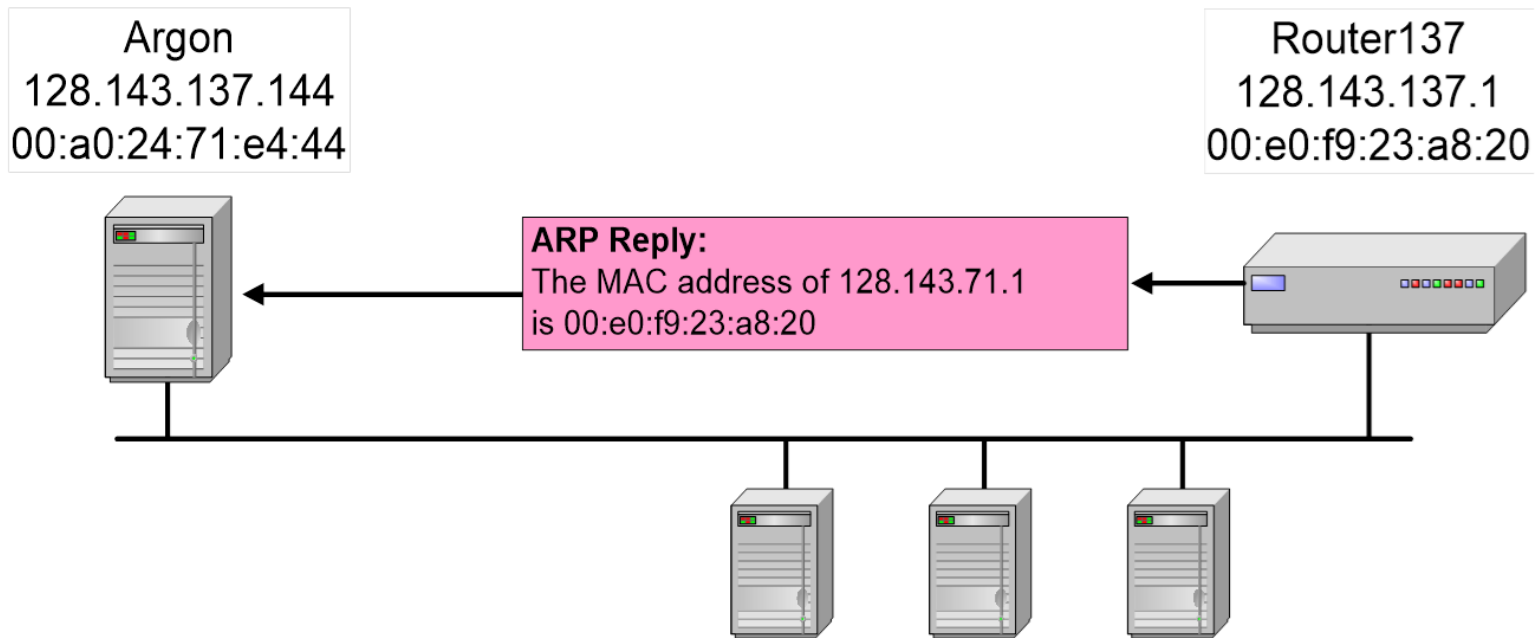
Argon στέλνει (broadcasts) ένα ARP ένα μήνυμα σε όλους τους σταθμούς του δικτύου με το περιεχόμενο: **“What is the hardware address of Router137?”**



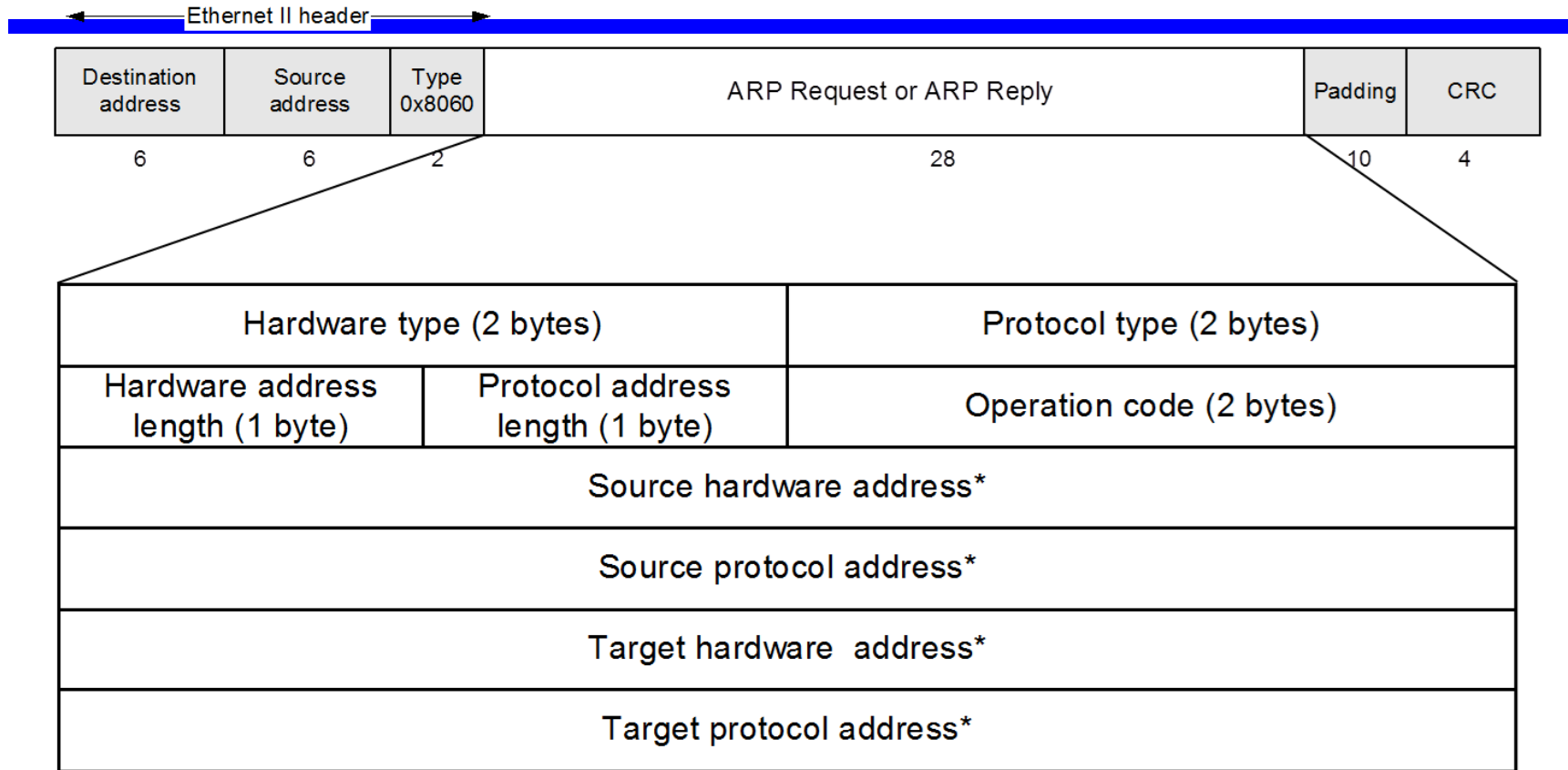
2-4. Φυσικές διευθύνσεις (ARP)

ARP Reply:

Router 137 απαντά με ένα ARP Reply το οποίο περιέχει την MAC διεύθυνση.



2-4. Φυσικές διευθύνσεις (ARP)



* Note: The length of the address fields is determined by the corresponding address length fields

2-4. Φυσικές διευθύνσεις (ARP)

- *ARP Request from Argon:*

Source hardware address:	00:a0:24:71:e4:44
Source protocol address:	128.143.137.144
Target hardware address:	00:00:00:00:00:00
Target protocol address:	128.143.137.1

- *ARP Reply from Router137:*

Source hardware address:	00:e0:f9:23:a8:20
Source protocol address:	128.143.137.1
Target hardware address:	00:a0:24:71:e4:44
Target protocol address:	128.143.137.144

2-4. Φυσικές διευθύνσεις (ARP)

- Λόγω του ότι η αποστολή πολλαπλών ARP request/reply από κάθε δικτυακή εφαρμογή είναι αναποτελεσματική, οι hosts διατηρούν κάθε replay στη μνήμη(ARP Cache) (20 min)
- Περιεχόμενα της ARP Cache:
 - (128.143.71.37) at 00:10:4B:C5:D1:15 [ether] on eth0
 - (128.143.71.36) at 00:B0:D0:E1:17:D5 [ether] on eth0
 - (128.143.71.35) at 00:B0:D0:DE:70:E6 [ether] on eth0
 - (128.143.136.90) at 00:05:3C:06:27:35 [ether] on eth1
 - (128.143.71.34) at 00:B0:D0:E1:17:DB [ether] on eth0
 - (128.143.71.33) at 00:B0:D0:E1:17:DF [ether] on eth0

2-4. Φυσικές διευθύνσεις (ARP)

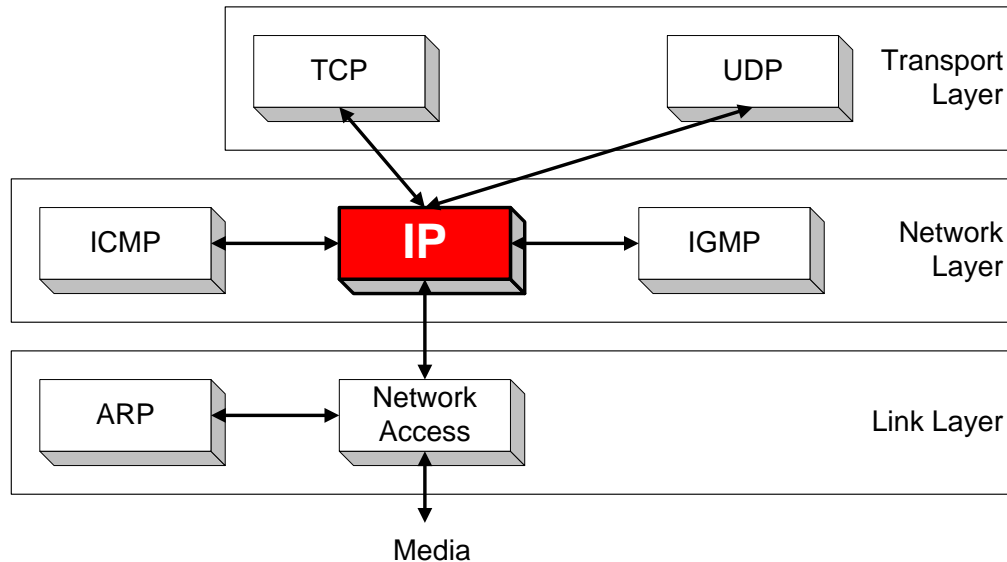
- Τι συμβαίνει την περίπτωση που δημιουργηθεί ARP request για ανύπαρκτη mac?

Επαναληπτικές αποστολές με αυξανόμενο χρονικό βήμα και παύση.
- Τι θα συμβεί αν ένας host στείλει ARP request για την δική του IP address?

Το πρωτόκολλο θα λειτουργήσει κανονικά. Αν λάβει απάντηση αυτό θα σημαίνει ότι η IP address έχει αποδοθεί σε περισσότερους του ενός Η/Υ.

3-1. Δομή πακέτου IP

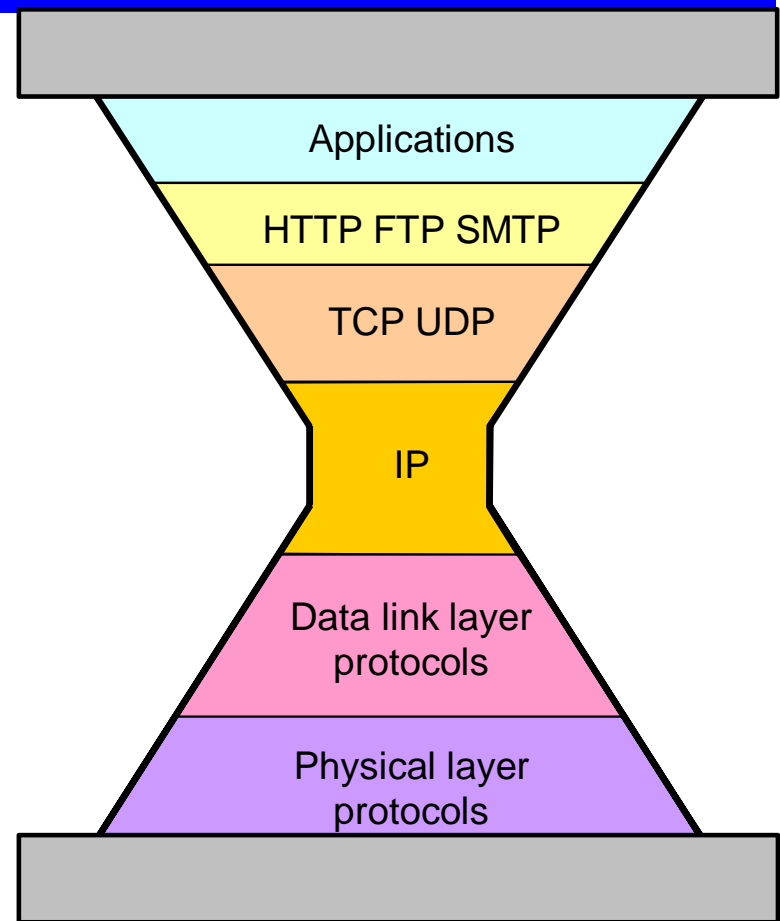
- IP (Internet Protocol) είναι πρωτόκολλο δρομολόγησης και ανήκει επίπεδο Δικτύου.



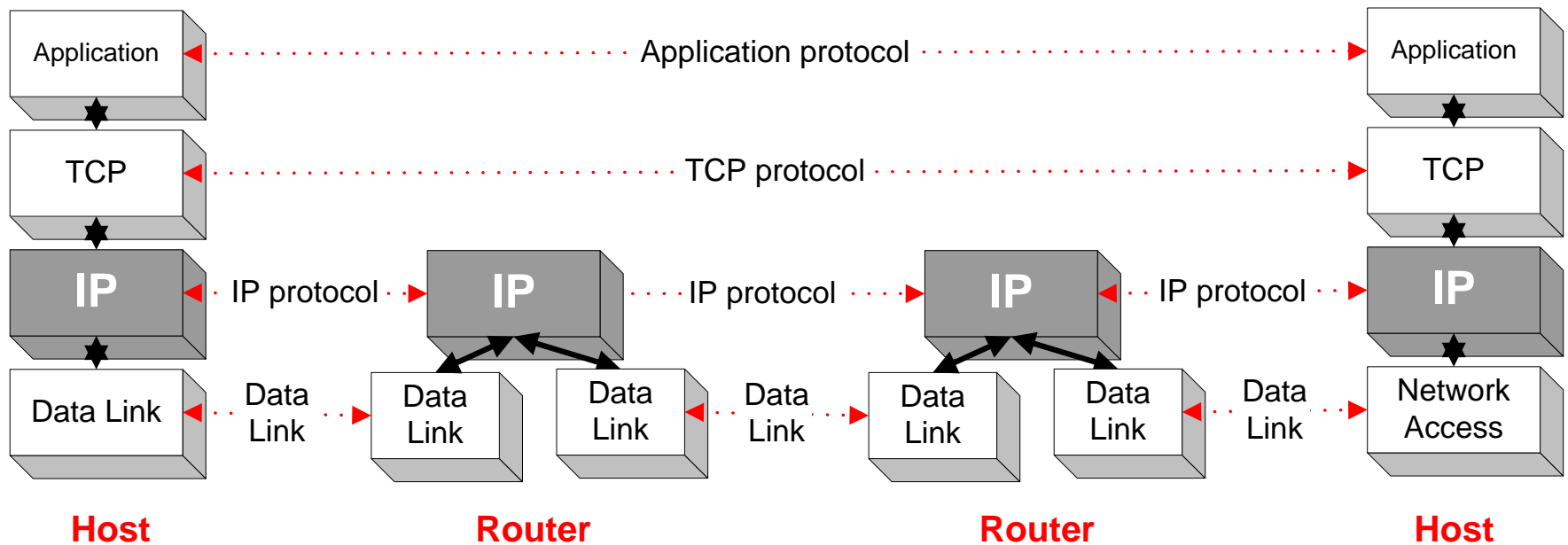
- IP Version 4 (IPv4) είναι ορισμένη στο RFC 891.

3-1. Δομή πακέτου IP

- Το IP αποτελεί την συνεκτική «ουσία» του Διαδικτύου.
- Πολλαπλά υψηλού - επιπέδου πρωτόκολλα
- Πολλαπλά χαμηλού - επιπέδου πρωτόκολλα
- Αλλά μόνο ένα πρωτόκολλο σε επίπεδο Δικτύου.



3-1. Δομή πακέτου IP



3-1. Δομή πακέτου IP

- Δρομολόγηση Πακέτων Δεδομένων
- IP παρέχει μη-αξιόπιστη μετάδοση δεδομένων (datagrams) στο Διαδίκτυο
 - **Unreliable:** δεν ανιχνεύει – διορθώνει λάθη.
 - **Connectionless:** είναι πιθανό κάθε πακέτο να ακολουθεί διαφορετικό δρόμο προς τον προορισμό.
 - **Best effort:** Δεν παρέχει ελάχιστες εγγυήσεις ποιότητας υπηρεσιών (no throughput guarantee, no delay guarantee,...)
- Μειονεκτήματα:
 - Τα πρωτόκολλα ανώτερου επιπέδου επιφορτίζονται να χειριστούν περιπτώσεις απωλειών πακέτων ή πολλαπλών λήψεων.
 - Η σειρά άφιξης των πακέτων διαφέρει από την σειρά εκπομπής.

3-2. Φόρμα πακέτου IP

0	4	8	16	19	24	31
Version	IHL	ToS	Total Length			
Identification			R	DF	MF	Fragment Offset
TTL		Protocol	Header Checksum			
Source Address						
Destination Address						
Options (Variable)						
Data (Variable)						

- $20 \text{ bytes} \leq \text{Header Size} < 2^4 \times 4 \text{ bytes} = 60 \text{ bytes}$
- $20 \text{ bytes} \leq \text{Total Length} < 2^{16} \text{ bytes} = 65536 \text{ bytes}$

3 – δομή

3-2. Φόρμα πακέτου IP

- **Version (4 bits):** υποστηρίζονται δύο εκδόσεις IPv4 και IPv6.
- **Header length (4 bits):** Μήκος του IP header, σε πολλαπλάσια των 4 bytes
- **Identification (16 bits):** Μοναδικός αριθμός που ορίζεται από τον αποστολέα και αυξάνεται σε κάθε νέα μετάδοση.
- **Flags (3 bits):**
 - First bit always set to 0
 - DF bit (Do not fragment)
 - MF bit (More fragments)Χρησιμοποιούνται και τον κερματισμό και την επανένωση των πακέτων.

3-2. Φόρμα πακέτου IP

- **Time To Live (TTL) (1 byte):**

- Ορίζει το μέγιστο μήκος διαδρομής που μπορεί να διανύσει ένα πακέτο στο Διαδίκτυο.
- Role of TTL field: Εξασφαλίζει τους «πόρους» του δικτύου.

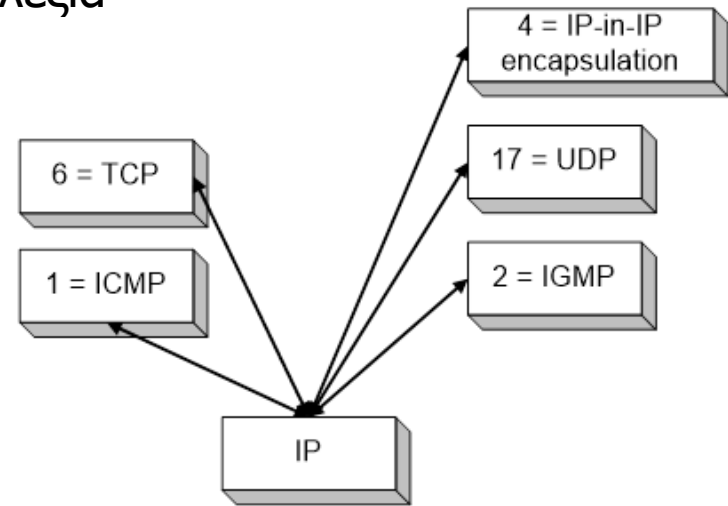
Χρησιμοποιείται ως εξής:

- Ο αποστολέας θέτει μια τιμή (e.g., 64)
- Κάθε δρομολογητής την μειώνει κατά 1
- Όταν το TTL γίνει 0, τότε το πακέτο απορρίπτεται.

3-2. Φόρμα πακέτου IP

- **Protocol (1 byte):**

- Καθορίζει το higher-layer protocol.
- Χρησιμοποιείται στην από-πολυπλεξία στα higher layers.



- **Header checksum (2 bytes):** checksum μήκους 16-bit επί της κεφαλίδας του IP πακέτου.

3-2. Φόρμα πακέτου IP

- **Options:**
 - Security restrictions
 - Record Route.
 - Timestamp
 - (loose) Source Routing: specifies a list of routers that must be traversed.
 - (strict) Source Routing: specifies a list of the only routers that can be traversed.
- **Padding:** Padding bytes are added to ensure that header ends on a 4-byte boundary

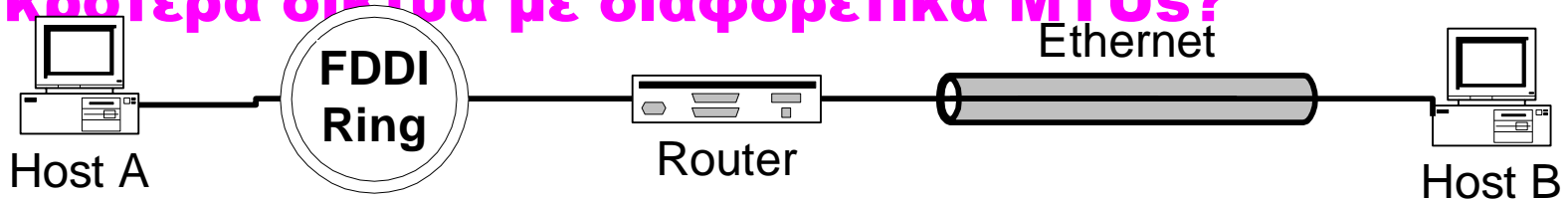
3-2. MTU

- Το μέγιστο δυνατό μέγεθος ενός IP datagram είναι 65535, αλλά το επίπεδο Δεδομένων (data link layer) καθορίζει το τελικό μέγεθός του πακέτου.
- Παράδειγμα:
 - Ethernet frames έχουν μέγιστο payload 1500 bytes
→ Αν τα IP datagrams ενθυλακωθούν σε Ethernet frames, τότε δεν μπορεί να είναι μεγαλύτερα από 1500 bytes
- Το μέγιστο όριο ενός IP datagram, ορίζεται από το πρωτόκολλο του data link και ονομάζεται **maximum transmission unit (MTU)**
- **MTUs για διάφορα data link protocols:**

Ethernet:	1500	FDDI:	4352
802.3:	1492	ATM AAL5:	9180
802.5:	4464	PPP:	negotiated

3-2. Fragmentation

- Αν το μέγεθος των δεδομένων IP datagram υπερβαίνει MTU?
- Αν το δίκτυο αποτελείται από ετερογενή μικρότερα δίκτυα με διαφορετικά MTUs?



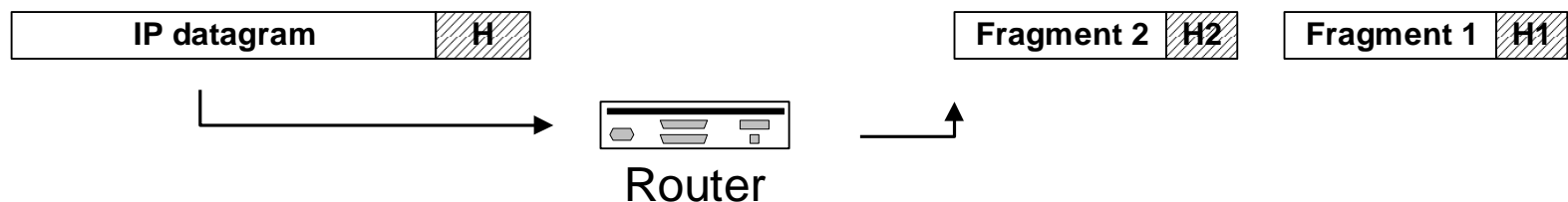
MTUs: **FDDI: 4352**

Ethernet: 1500

- **Fragmentation:**
- IP το datagram κερματίζεται άλλα μικτότερου μεγέθους.
- Ο παραλήπτης αναλαμβάνει την επανένωση τους.

3-2. Fragmentation

- Fragmentation μπορεί να γίνει στον αποστολέα ή σε κάποιο ενδιάμεσο router.
- Το ίδιο datagram μπορεί να υποστεί κερματισμό παραπάνω από μια φορές.
- Η επανένωση γίνεται μόνο στον παραλήπτη!! (γιατί??)



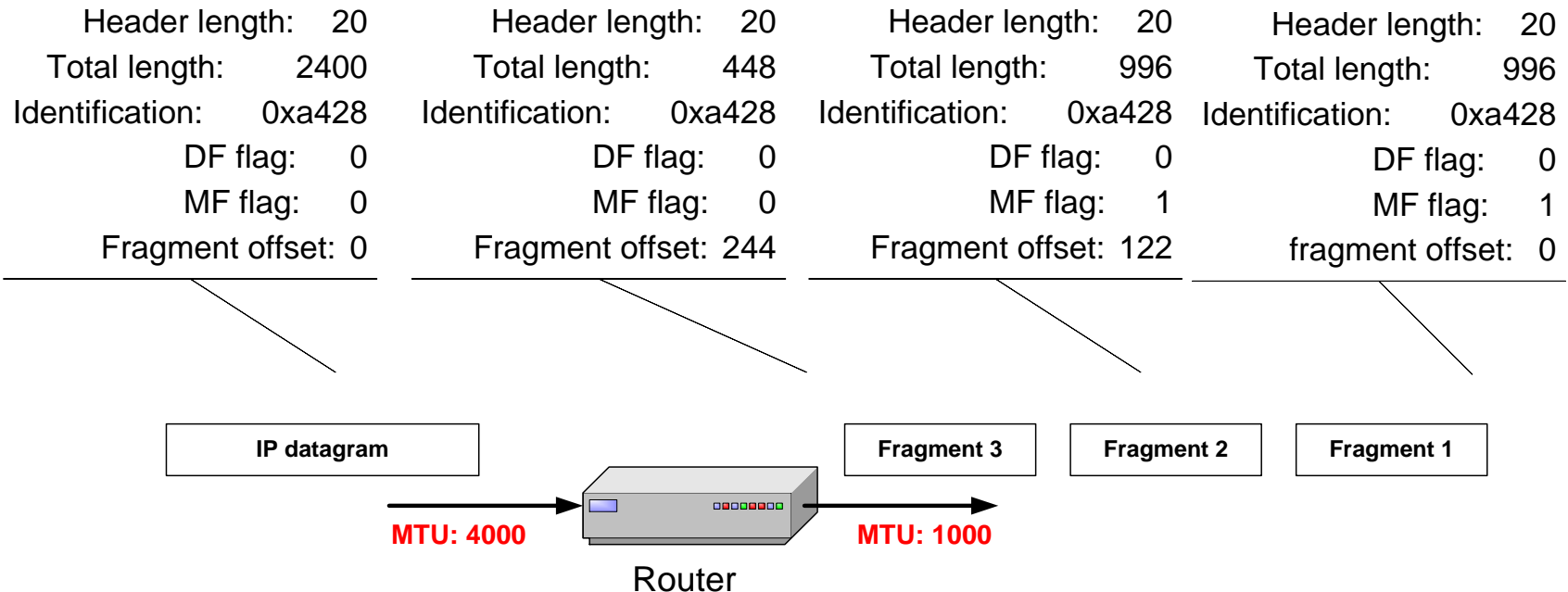
3-2. Fragmentation

- Εμπλέκονται τα εξής πεδία:

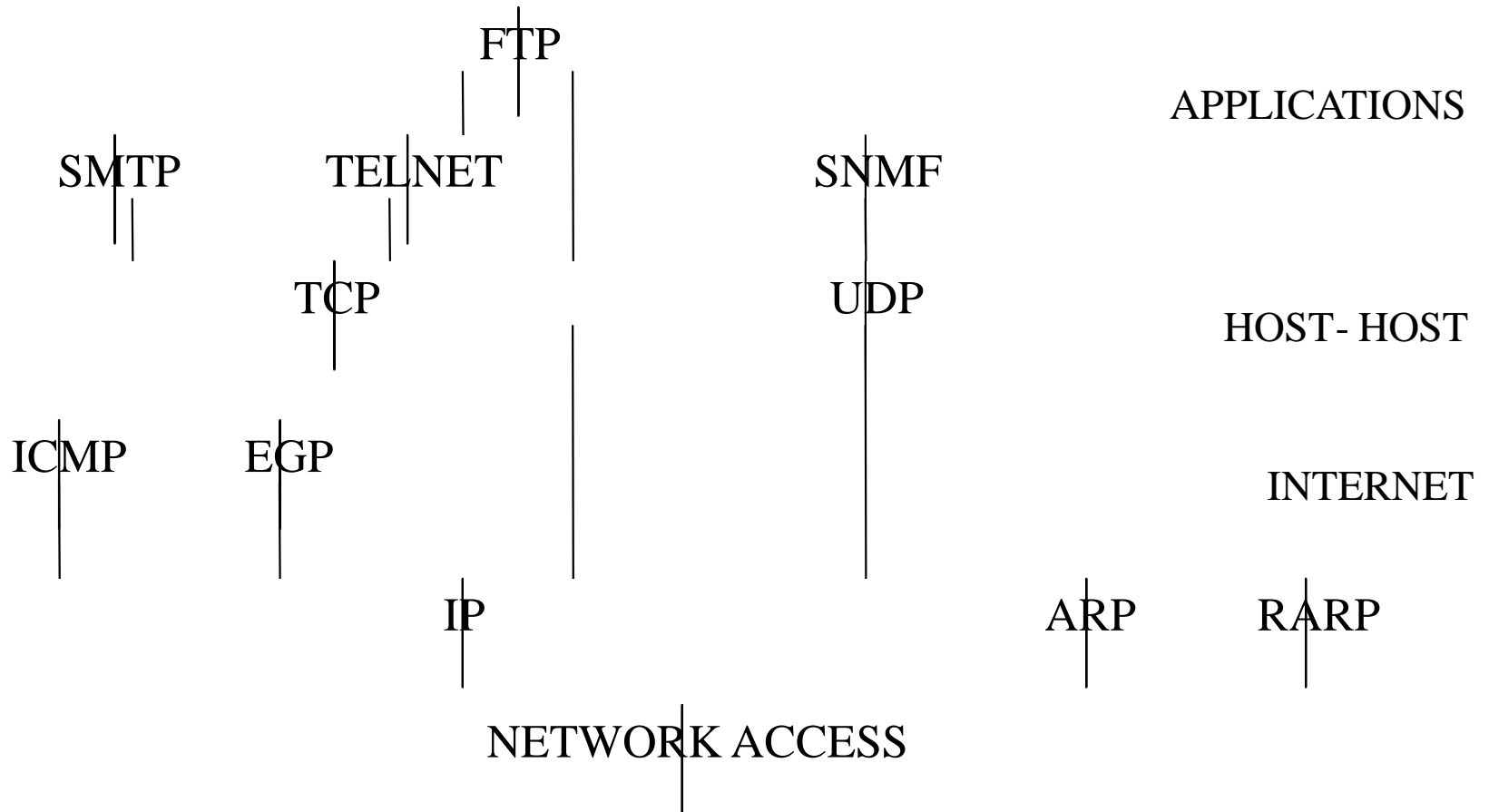
version	header length	DS	ECN	total length (in bytes)			
Identification				0	D F	M F	Fragment offset
time-to-live (TTL)	protocol		header checksum				

3-2. Fragmentation

- Ένα datagram μεγέθους 2400 bytes πρέπει να κερματιστεί έτσι ώστε να περάσει από δίκτυο με MTU limit 1000 bytes



3-3. Πρωτόκολλα Διαδικτύου



4-1. Τεμαχισμός

- Αναγκαίος όταν δρομολογητής πρέπει να στείλει σε δίκτυο με μικρότερη (MTU-Max Transfer Unit)
- Κάθε πακέτο έχει ταυτότητα (identification number) και σημαία MF (More Fragments) που δείχνει εάν είναι τελευταίο ή μοναδικό τεμάχιο, όταν MF=0.
- Τεμάχια ιδίου πακέτου κρατούν ίδιο identification No
- Το πεδίο offset (bytes από αρχή) δείχνει θέση τεμαχίου
- Τελευταίο τεμάχιο παίρνει σημαία MF=0, τα άλλα MF=1
- Σημαία DF απαγορεύει τεμαχισμό
- Τεμαχισμένο πακέτο δεν ξανασυναμολογείται σε ενδιάμεσους δρομολογητές, μόνο στο τερματικό.

4-2. Παράδειγμα τεμαχισμού

DATAGRAM HEADER	Data 2000octets
--------------------	--------------------

FRAGMENT 1 HEADER	Data 1 800octets
----------------------	---------------------

Fragment 1 (offset 0)

FRAGMENT 2 HEADER	Data 1 800octets
----------------------	---------------------

Fragment 2 (offset 800)

FRAGMENT 3 HEADER	Data 3 400oct
----------------------	------------------

Fragment 3 (offset 1600)

4-3. Συναρμολόγηση

- Γίνεται μόνο στον τελικό προορισμό
- Εάν δεδομένογραμμα έχει $offset=0$ και $MF=1$ ή $MF=0$ αλλά $offset \neq 0$, τότε είναι τεμάχιο άλλου μεγαλύτερου
- Μηχανή συναρμολόγησης ανά identification number διότι τεμάχια ιδίου πακέτου έχουν ίδιο identification No
- Πρώτο το τεμάχιο με $offset=0$
- Ακολουθεί το τεμάχιο με $offset=$ μήκος προηγούμενου τεμαχίου (ίδιο Id No και $MF=1$)
- Συναρμολόγηση τελειώνει όταν βρεθεί τεμάχιο με σημαία $MF=0$

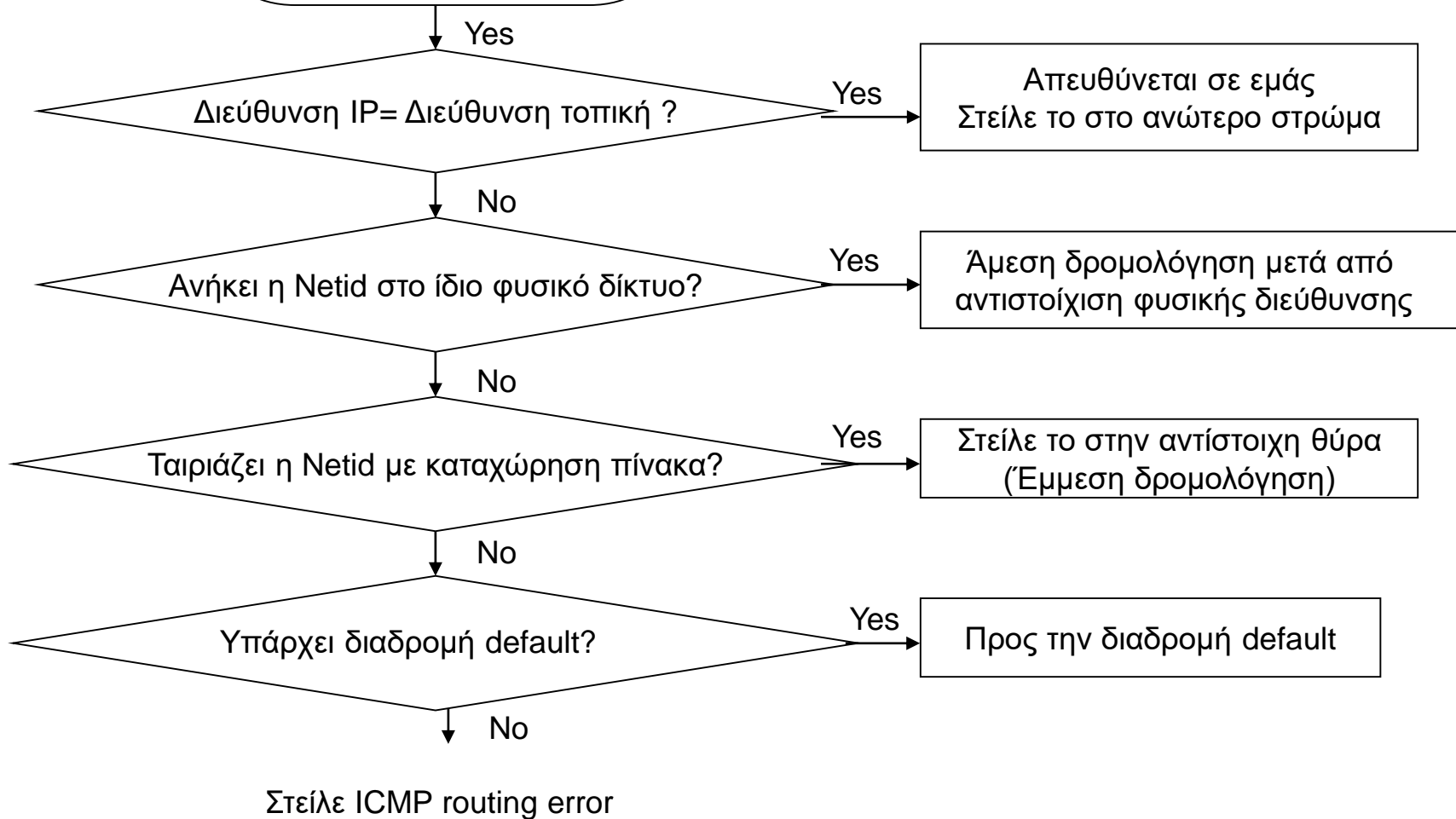
5-1. Δρομολόγηση

Δύο κύριες λειτουργίες:

- Αποθήκευση-Προώθηση (store & Forward)
 - Εντοπισμός καταχώρησης διεύθυνσης σε πίνακα δρομολόγησης και αντίστοιχης πόρτας εξόδου
 - Προώθηση πακέτου στην θύρα
 - Λαμβάνει χώρα χιλιάδες φορές ανά δευτ/πτο
- Εύρεση τοπολογίας (topology discovery)
 - Συνεχής εκτέλεση στο φόντο (background) αλγορίθμου βελτιστοποίησης διαδρομών (π.χ. Dijkstra) με ανταλλαγές ανά λίγα δευτ. πληροφοριών μεταξύ δρομολογητών

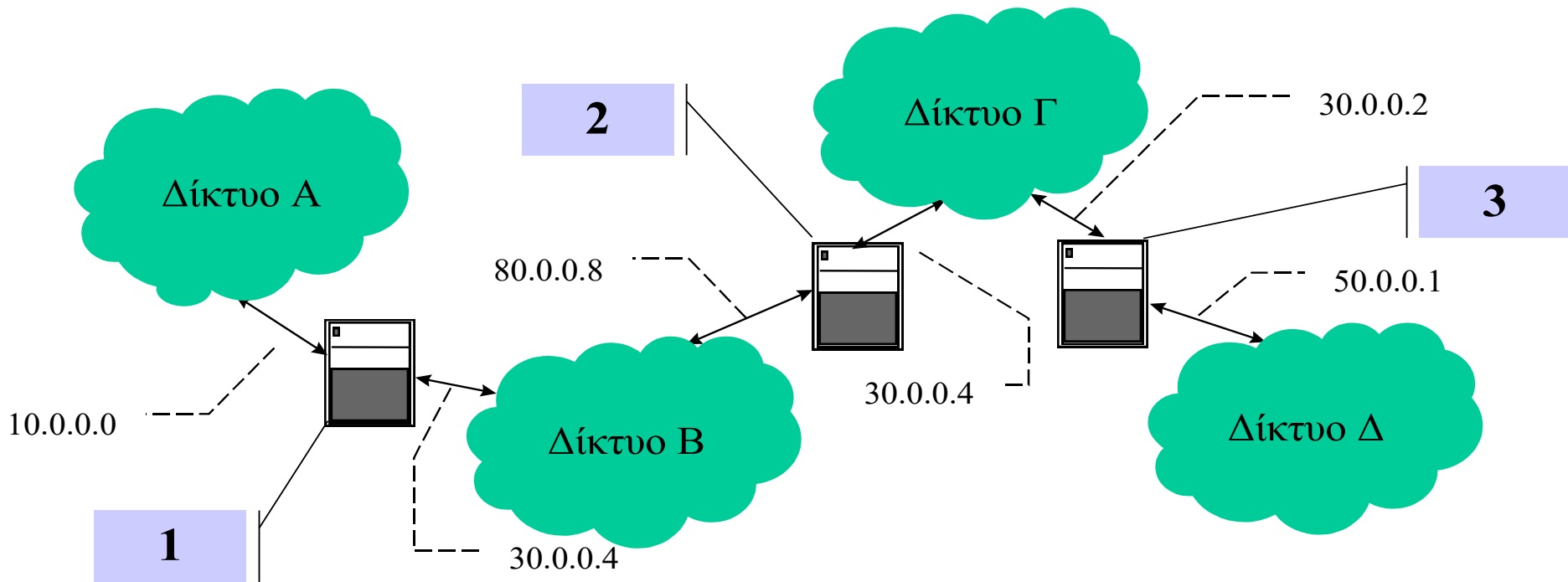
5-2. Αλγόριθμος Δρομολόγησης

Εισερχόμενο πακέτο



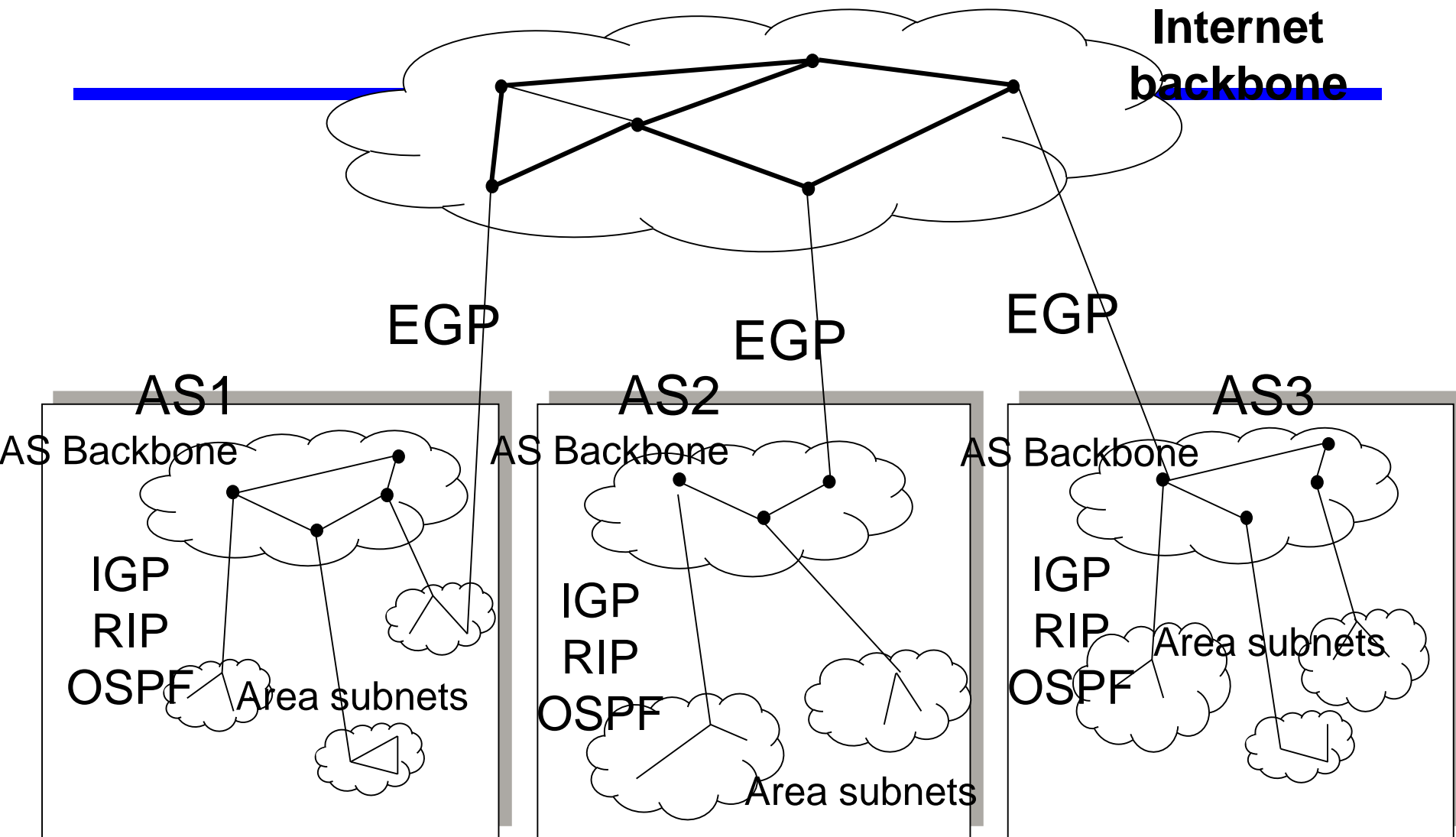
5-3. Εμεση & Άμεση Δρομολόγηση

Για ένα πακέτο από το Δίκτυο Α στο Δ, οι δρομολογητές 1 και 2 θα κάνουν έμμεση δρομολόγηση (προώθηση στον επόμενο βάσει πίνακα) αλλά ο 3 άμεση με χρήση ARP



6-1. Επιλογή διαδρομών

- Η εύρεση πόρτας εξόδου στον πίνακα προσδιορίζει την διαδρομή του πακέτου στο τρέχον βήμα.
- Η καταχώριση προκύπτει από βελτιστοποίηση των διαδρομών που λαμβάνει χώρα με εκτέλεση σε συνεργασία μεταξύ των κόμβων και με κατανεμημένο τρόπο αλγορίθμων εύρεσης τοπολογίας.
- Ενιαίος αλγόριθμος σε κάθε διοικητικά αυτόνομο σύστημα (π.χ. OSPF, RIP, IGP)
- Διαφορετικοί αλγόριθμοι μεταξύ αυτόνομων συστημάτων (π.χ. EGP)



6 – Επιλογή διαδρομών

ASx: Autonomous System

Ι. Δ. Αγγελόπουλος,
καθηγητής

6-3. Πρωτόκολλα - Επιλογή διαδρομών

Εσωτερικά στα ΑΣ χρησιμοποιούνται τα πρωτόκολλα:

RIP: Routing Information Protocol (χρησιμοποιεί τον αλγόριθμο Bellman-Ford)

• **OSPF: Open Shortest Path First**
(χρησιμοποιεί τον αλγόριθμο Dijkstra)

Εξωτερικά μεταξύ διαφορετικών ΑΣ χρησιμοποιείται το πρωτόκολλο:

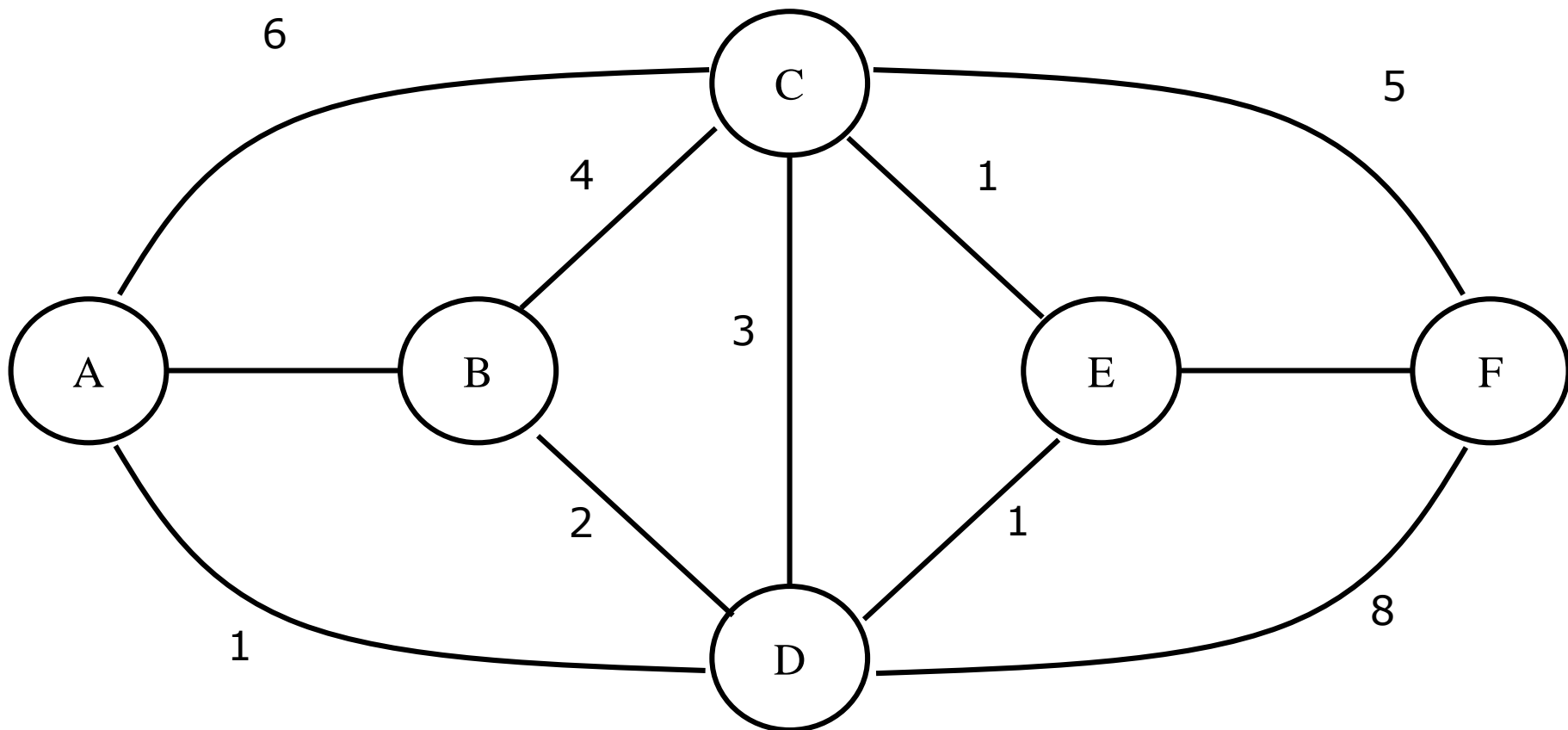
• **EGP: Exterior Gateway Protocol**

Στη συνέχεια αναλύεται ο αλγόριθμος Dijkstra

7-1. Βήματα Αλγορίθμου Dijkstra

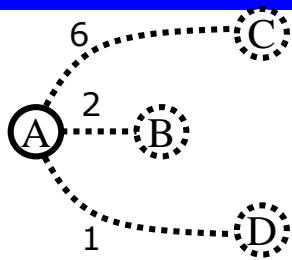
1. Να ανακαλύπτει τους γείτονές του και να μαθαίνει τις διευθύνσεις δικτύου τους
2. Να υπολογίζει την καθυστέρηση ή το κόστος για καθέναν από τους γείτονές του
3. Να κατασκευάζει ένα πακέτο που πληροφορεί όλα αυτά που μόλις έμαθε
4. Να στέλνει το πακέτο προς όλους τους δρομολογητές
5. Να υπολογίζει τη συντομότερη διαδρομή προς κάθε άλλον δρομολογητή.

7-2. Τοπολογία παραδείγματος Dijkstra



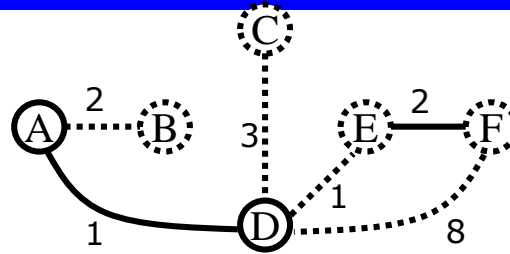
Αρχικοποίηση (1η επαν/ψη)

$$M = \{A\}$$



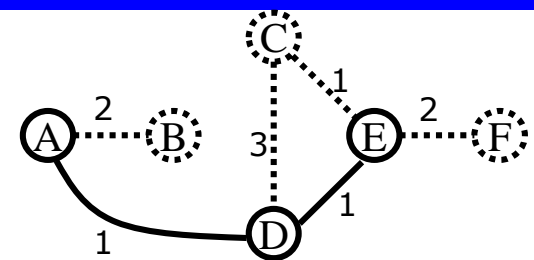
2η επανάληψη

$$M = \{A, D\}$$



3η επανάληψη

$$M = \{A, D, E\}$$



Αρχικό κόστος διαδρομών από A

$K_B = 2$ μέσω διαδρομής A-B

$K_C = 6$ μέσω διαδρομής A-C

$K_D = 1$ μέσω διαδρομής A-D

$K_E = (\text{άπειρο})$

$K_F = (\text{άπειρο})$

Νέο κόστος διαδρομών από A

$K_B = 2$ μέσω διαδρομής A-B

$K_C = 4$ μέσω διαδρομής A-D-C*

$K_D = 1$ μέσω διαδρομής A-D

$K_E = 2$ μέσω διαδρομής A-D-E*

$K_F = 9$ μέσω διαδρομής A-D-E*

Νέο κόστος διαδρομών από A

$K_B = 2$ μέσω διαδρομής A-B

$K_C = 3$ μέσω διαδρομής A-D-E-C*

$K_D = 1$ μέσω διαδρομής A-D

$K_E = 2$ μέσω διαδρομής A-D-E

$K_F = 4$ μέσω διαδρομής A-D-E-F*

Βήμα 1: Βρες γείτονα με min κόστος (Απ. D)

Βήμα 2: Πρόσθεση του D στο σύνολο M και μετά επανάληψη ενημέρωσης πίνακα κόστους

Βήμα 1: Νέος γείτονας με min κόστος (Απ. B, E έστω E)

Βήμα 2: Πρόσθεση του E στο σύνολο M και 3η επανάληψη ενημέρωσης πίνακα κόστους

Βήμα 1: Νέος γείτονας με min κόστος (Απ. B)

Βήμα 2: Πρόσθεση του B στο σύνολο M και 4η επανάληψη ενημέρωσης πίνακα κόστους

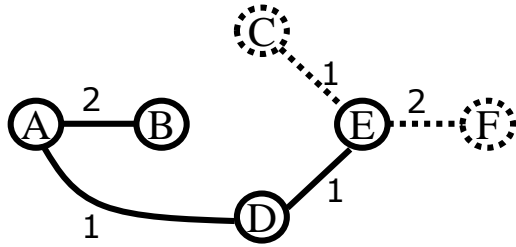
7 – αλγόριθμοι

*Ο αστερίσκος δείχνει βελτίωση κόστους μέσω του νέου κόμβου

Ι. Δ. Αγγελόπουλος,
καθηγητής

4η επανάληψη

$M = \{A, B, D, E\}$



Νέο κόστος διαδρομών από A

$K_B = 2$ μέσω διαδρομής A-B

$K_C = 3$ μέσω διαδρομής A-D-E-C

$K_D = 1$ μέσω διαδρομής A-D

$K_E = 2$ μέσω διαδρομής A-D-E

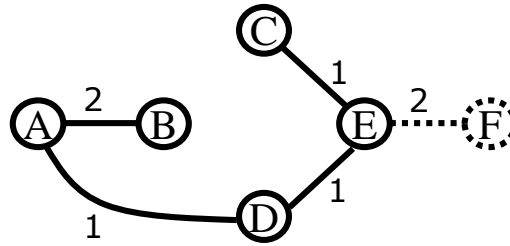
$K_F = 4$ μέσω διαδρομής A-D-E-F

Βήμα 1: Νέος γείτονας με min κόστος (Απ. C)

Βήμα 2: Πρόσθεση του στο σύνολο M και 5η επανάληψη ενημέρωσης πίνακα κόστους

5η επανάληψη

$M = \{A, B, C, D, E\}$



Νέο κόστος διαδρομών από A

$K_B = 2$ μέσω διαδρομής A-B

$K_C = 3$ μέσω διαδρομής A-D-E-C

$K_D = 1$ μέσω διαδρομής A-D

$K_E = 2$ μέσω διαδρομής A-D-E

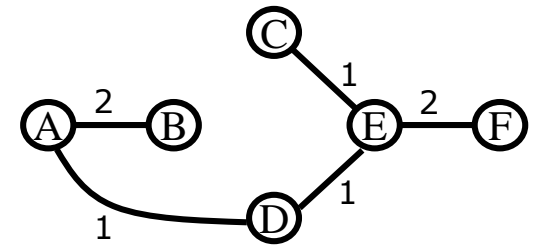
$K_F = 4$ μέσω διαδρομής A-D-E-F

Βήμα 1: Νέος γείτονας (και τελευταίος) με min κόστος: E

Βήμα 2: Πρόσθεση του στο σύνολο M και 6η επανάληψη ενημέρωσης πίνακα κόστους

6η επανάληψη

$M = \{A, B, C, D, E, F\}$



Νέο κόστος διαδρομών από A

$K_B = 2$ μέσω διαδρομής A-B

$K_C = 3$ μέσω διαδρομής A-D-E-C

$K_D = 1$ μέσω διαδρομής A-D

$K_E = 2$ μέσω διαδρομής A-D-E

$K_F = 4$ μέσω διαδρομής A-D-E-F

(Ουδεμία αλλαγή)

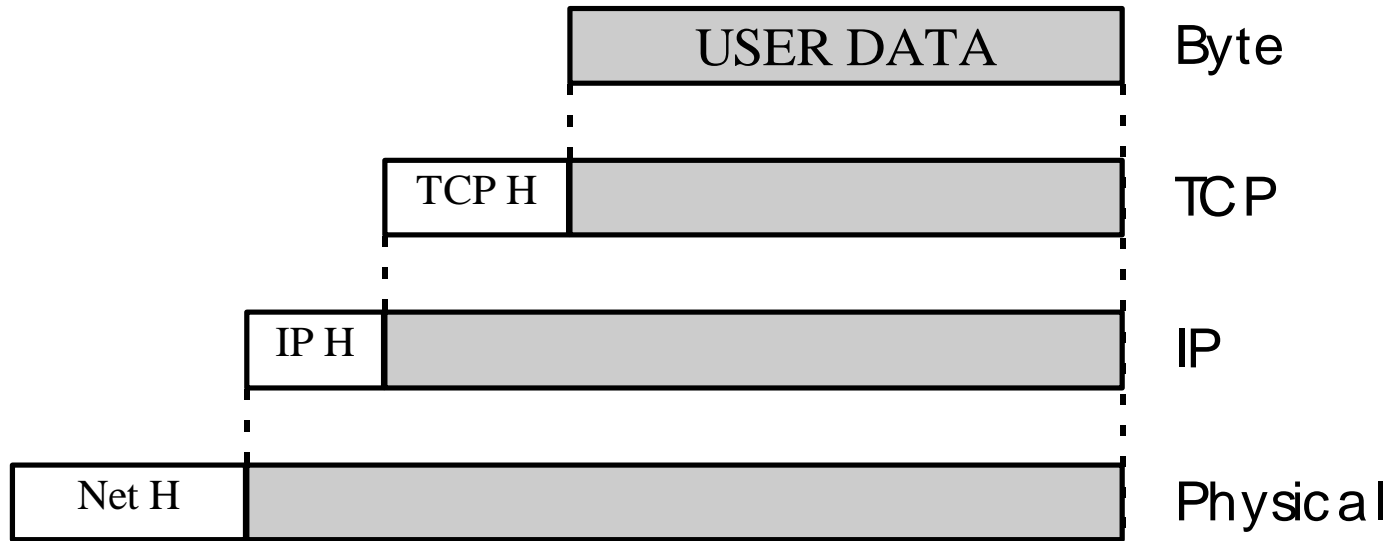
Έχουν ενταχθεί στο M όλοι οι κόμβοι και άρα αυτό είναι το τελικό κόστος

Θα υπήρχε τελική διαφορά εάν είχαμε επιλέξει τον B πριν τον E μετά την 2η επανάληψη;

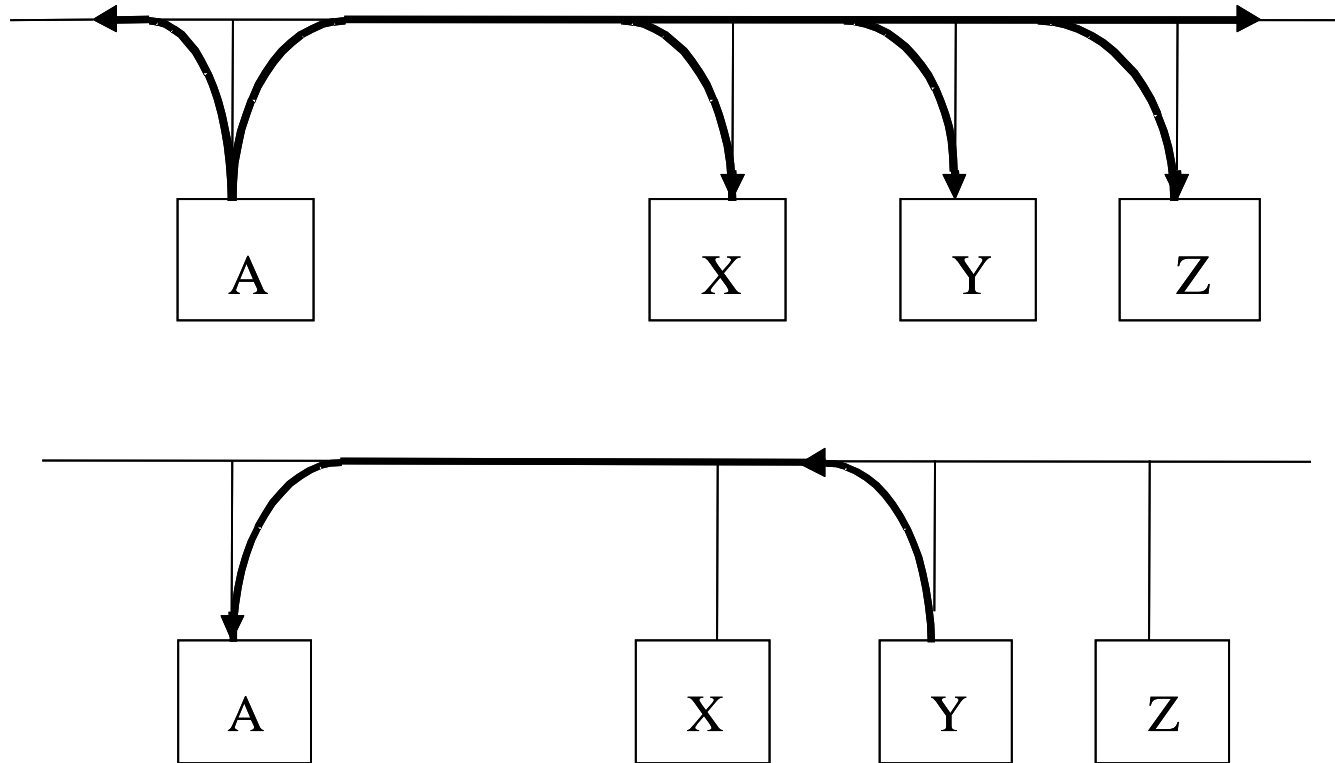
8-1. Ενθυλάκωση IP σε Ethernet

- Για διαβίβαση μέσω φυσικού δικτύου Ethernet το δεδομένογραμμα ενθυλακώνεται σε πλαίσιο Ethernet το οποίο είναι απαραίτητο για χειρισμό από μεταγωγείς και πλήμνες Ethernet (ιδέ σχήμα 8-2)
- Για σωστή διαβίβαση απαιτείται η αντιστοίχιση της διεύθυνσης MAC και IP του υπολογιστή προορισμού
- Αυτό επιτυγχάνεται μέσω πρωτοκόλλου ARP (Address Resolution Protocol) με μια ανταλλαγή μηνυμάτων που φαίνεται στο σχήμα 8-3
- Η φόρμα του μηνύματος ARP φαίνεται στο σχήμα 8-4

8-2. Ενθυλάκωση IP σε Ethernet



8-3. Ενθυλάκωση IP σε Ethernet



8-4. Φόρμα μηνύματος ARP

0	8	16	24	31
HARDWARE TYPE		PROTOCOL TYPE		
HLEN	PLEN	OPERATION		
SENDER HA (octets 0 - 3)				
SENDER HA (octets 4 - 5)		SENDER IP (octets 0 - 1)		
SENDER IP (octets 2 - 3)		TARGET HA (octets 0 - 1)		
TARGET HA (octets 2 - 5)				
TARGET IP (octets 0 - 3)				

9-1. ICMP

- Οι δρομολογητές του Διαδικτύου δρουν με βάση την βέλτιστη προσπάθεια (Best effort) αλλά χωρίς εγγυήσεις
- Όταν κάτι πάει στραβά απορρίπτουν το πακέτο χωρίς προσπάθεια επανόρθωσης (Το TCP αναλαμβάνει αυτό)
- Ωστόσο διαθέτουν το πρωτόκολλο ICMP (Internet Control Message Protocol) μέσω του οποίου ειδοποιούν τον αποστολέα για το πρόβλημα.
- Διαθέτει δική του φόρμα και τα μηνύματα του ενθυλακώνονται σε πακέτα IP
- Διαθέτει πεδίο 8 Bits όπου κωδικοποιεί τα μηνύματα

9-2. ICMP

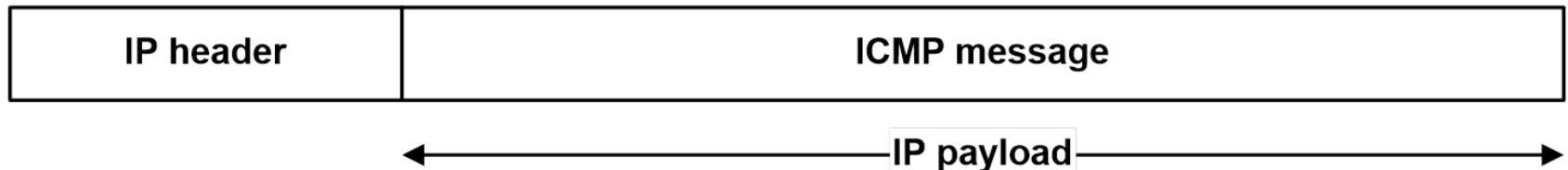
Μερικοί κωδικοί μηνυμάτων ICMP:

- 0 echo the reply
(χρησιμοποιείται στην γνωστή διαγνωστική εφαρμογή ping)
- 3 destination unreachable
- 4 source quench
- 5 redirect (change route)
- 11 “Time-to-Live” exceeded (χρησιμοποιείται στην γνωστή διαγνωστική εφαρμογή traceroute, όπου τίθενται διαδοχικά TTL = 1, 2, 3 κτλ, αναγκάζοντας διαδοχικά τους δρομολογητές να στείλουν το μήνυμα)

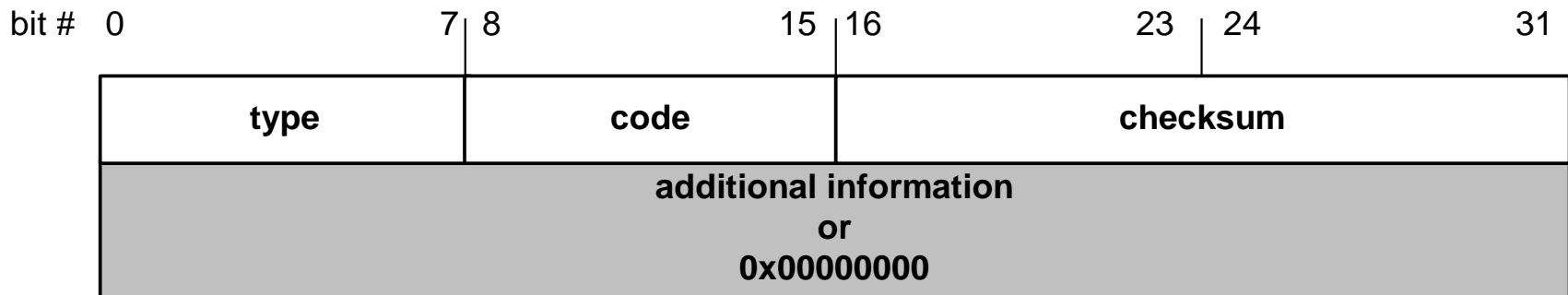
9-3. ICMP

Overview

- Το **Internet Control Message Protocol (ICMP)** είναι ένα βοηθητικό πρωτόκολλο το οποίο παρέχει:
 - Error reporting
 - Simple queries
- Τα ICMP μηνύματα είναι ενθυλακωμένα σε IP datagrams:



9-3. ICMP (Message format)



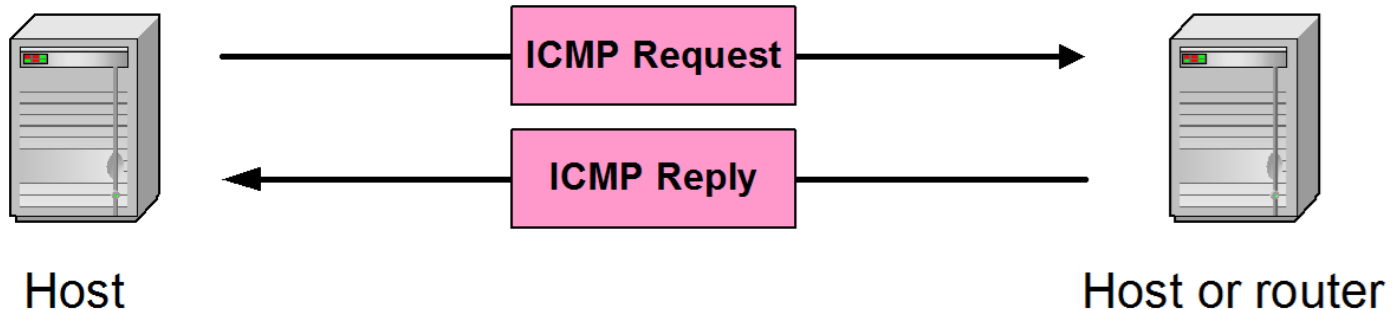
4 byte header:

- **Type (1 byte)**: type of ICMP message
- **Code (1 byte)**: subtype of ICMP message
- **Checksum (2 bytes)**: όπως το IP header checksum. Το Checksum υπολογίζεται πάνω σε όλο το ICMP μήνυμα.

Στην περίπτωση που δεν υπάρχουν επιπλέον δεδομένα, ακολουθούν 4 bytes με μηδενική τιμή.

→ κάθε ICMP message έχει ελάχιστο μήκος 8 bytes

9-3. ICMP



ICMP query:

- **Request** αποστέλλεται από ένα host προς κάποιο router ή άλλο host
- **Reply** αποστέλλεται στον host που έκανε το ερώτημα.

9-3. ICMP (Queries)

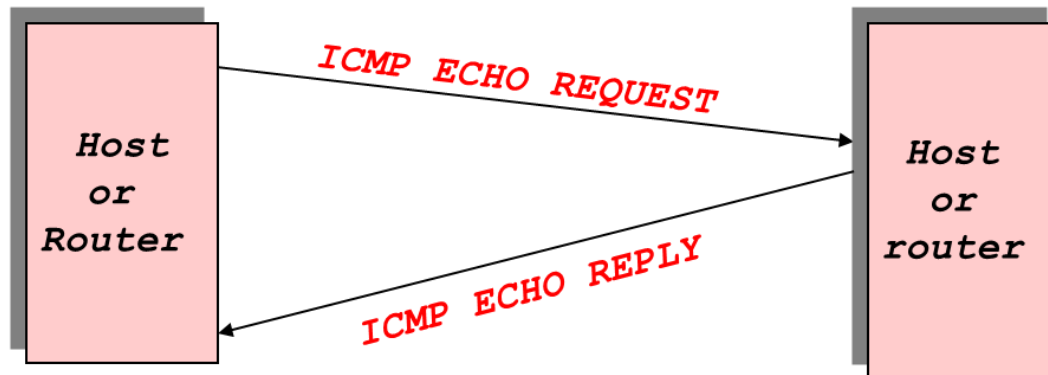
Type/Code:	Description
8/0	Echo Request
0/0	Echo Reply
13/0	Timestamp Request
14/0	Timestamp Reply
10/0	Router Solicitation
9/0	Router Advertisement



The ping command uses Echo Request/Echo Reply

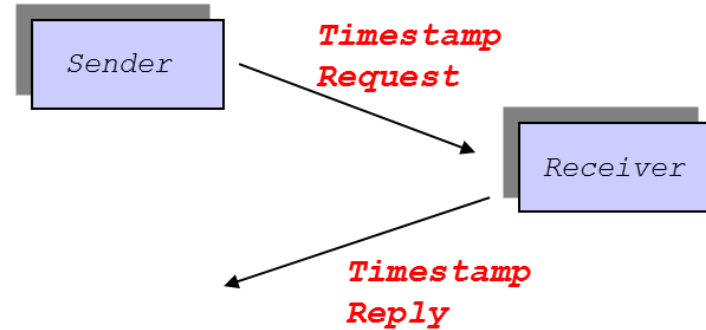
9-3. ICMP (Ping)

- Ping
- Κάθε Ping μεταφράζεται σε ένα **ICMP Echo Request**
- Οι hosts απαντούν με ένα **ICMP Echo Reply**



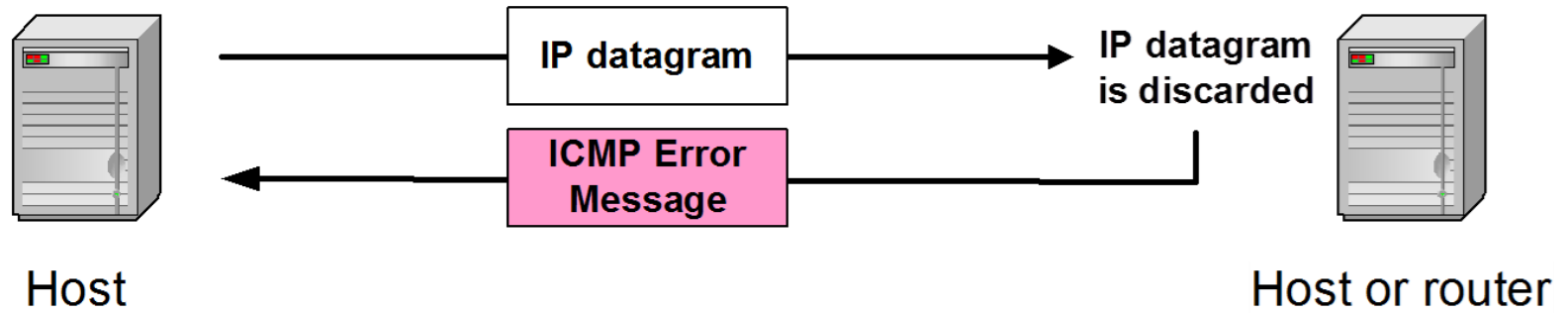
9-3. ICMP (Timestamp)

- Κάποιος (host or router) ρωτά την τρέχουσα τιμή χρόνου κάποιου άλλου (host or router).
- Ο χρόνος μετράται σε milliseconds UTC (Universal Coordinated Time)
- Ο αποστολέας στέλνει ένα **request**, και ο παραλήπτης απαντά με ένα **reply**



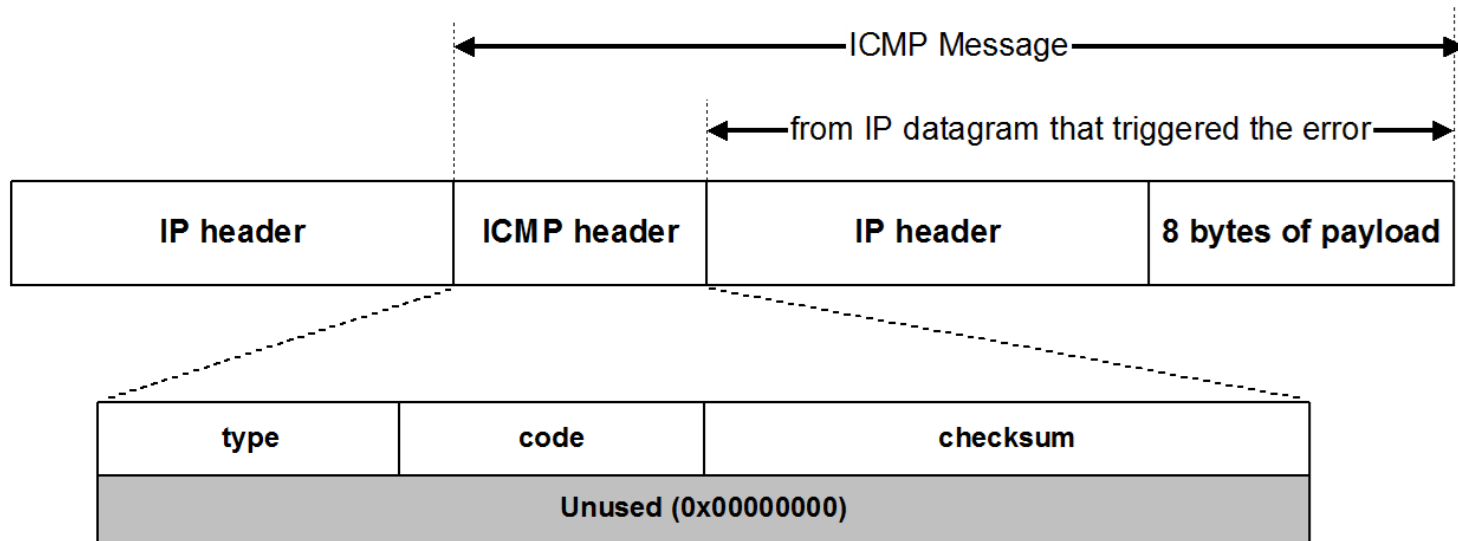
Type (= 17 or 18)	Code (=0)	Checksum
identifier		sequence number
32-bit sender timestamp		
32-bit receive timestamp		
32-bit transmit timestamp		

9-3. ICMP (Error)



- Στέλνονται όταν κάποιο datagram απορρίπτεται
- Τα ICMP μηνύματα σφάλματος συνήθως παραδίδονται στην δικτυακή εφαρμογή.

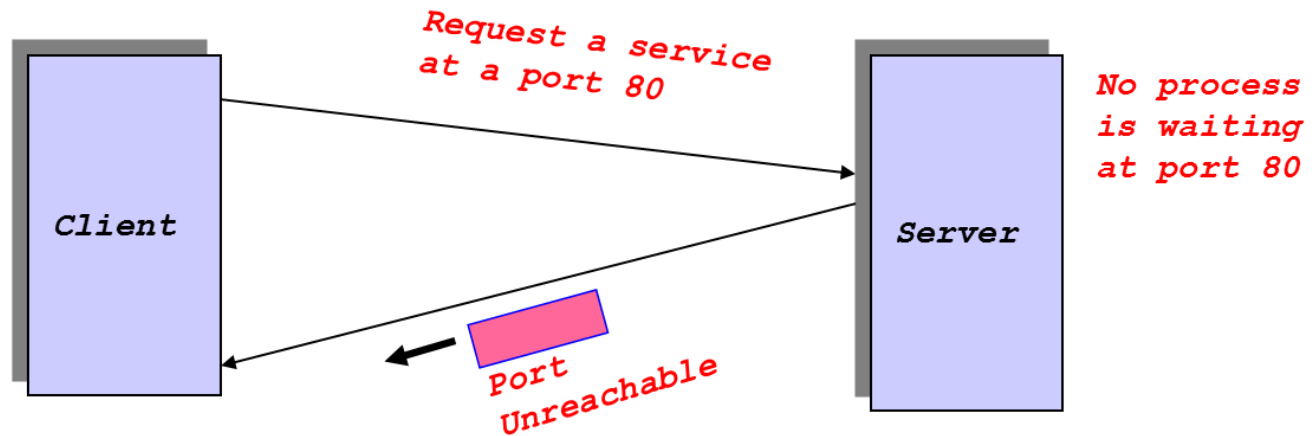
9-3. ICMP (Error)



- Τα ICMP error messages περιλαμβάνουν όλο το IP header και τα πρώτα 8 bytes από το payload (typically: UDP, TCP)

9-3. ICMP

- RFC 792: If, in the destination host, the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source host.
- Scenario:



9-3. ICMP

Type	Code	Description	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

9-3. ICMP

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

10-1. TCP

Το TCP παρέχει αξιόπιστη Υπηρεσία συνεχούς ροής bytes με αμφίδρομες νοητές συνδέσεις και χρήση τοπικού ταμιευτήρα

- **Αξιοπιστία:** ο αποστολέας και ο παραλήπτης ελέγχουν συνεχώς μέσω ελέγχου λαθών και θετικών επιβεβαιώσεων ότι δεν εχάθη ή διεφθάρη ούτε ένα Bit.
- Στη αντίθετη περίπτωση προβαίνουν σε άμεση διόρθωση του λάθους μέσω αναμετάδοσης του αλλοιωθέντος ή απωλεσθέντος πακέτου
- Γίνεται αρίθμηση πακέτων και έλεγχος ροής μέσω παραθύρου ολίσθησης
- Επίσης έλεγχος συμφόρησης μέσω έμμεσης ανίχνευσης απωλειών πακέτων και ειδικών αλγορίθμων

10-2. TCP

Το TCP παρέχει Υπηρεσία με νοητή σύνδεση
Δηλ. ο αποστολέας και ο παραλήπτης δημιουργούν ακραία σημεία, που ορίζονται από: διεύθυνση IP host + θύρα (port)
Η Θύρα είναι ένας τοπικός αριθμός 16 bit για κάθε host (65.536 θύρες).

Για να πάρουμε υπηρεσίες TCP, πρέπει πρώτα να εγκατασταθεί ρητά σύνδεση μεταξύ μιας υποδοχής του μηχανήματος αποστολής και μιας υποδοχής στο μηχάνημα λήψης

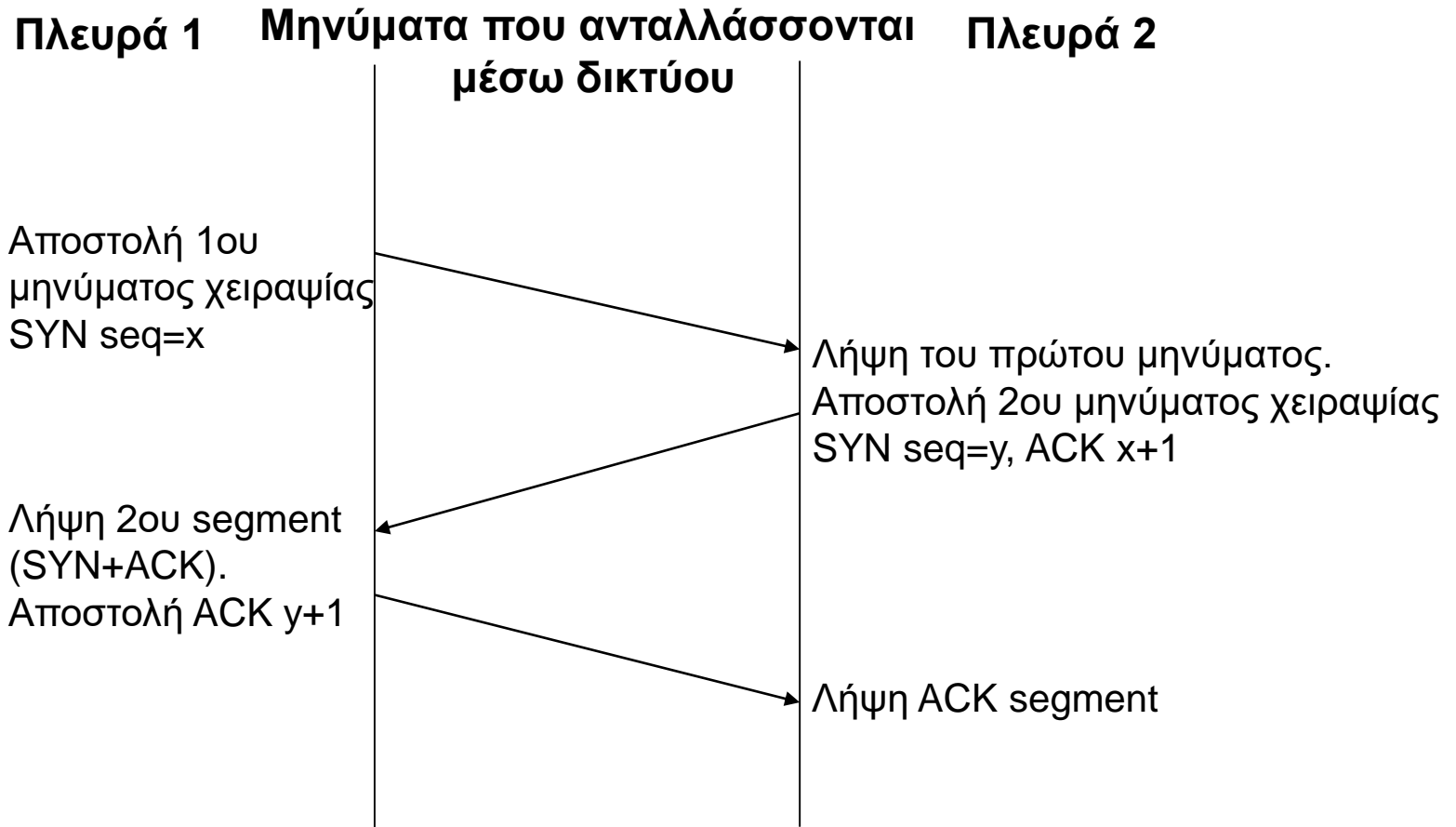
Η εφαρμογή και το TCP (που είναι δύο διαδικασίες λογισμικού) ανταλλάσσουν τα δεδομένα σε σημεία της μνήμης του ξενιστή που ονομάζονται υποδοχές (sockets)

10-3. Φόρμα TCP

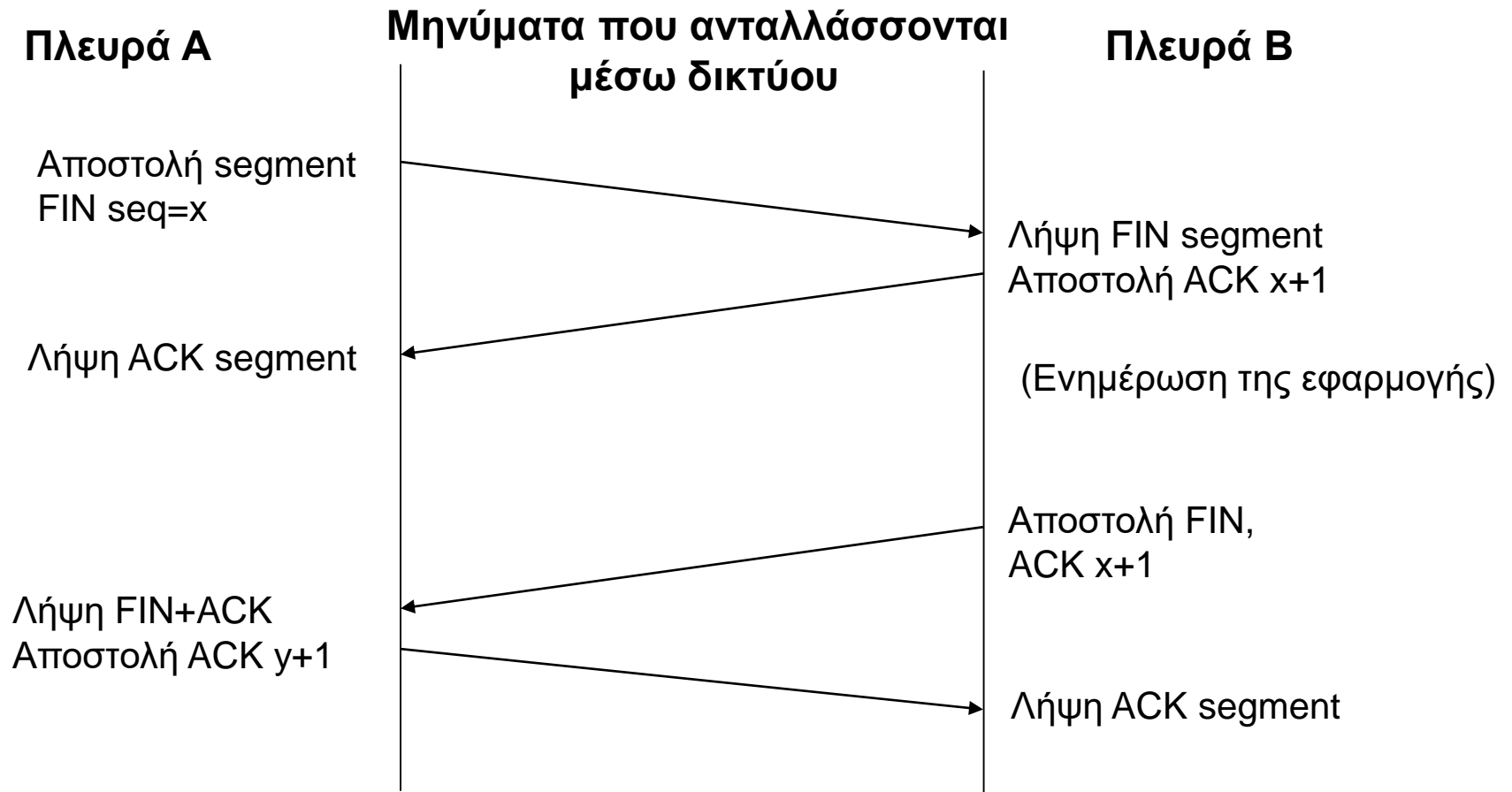
0 4 10 16 24 31

SOURCE PORT			DESTINATION PORT		
SEQUENCE NUMBER					
ACKNOWLEDGEMENT NUMBER					
HLEN	RESERVED	CODE BITS	WINDOW		
CHECKSUM			URGENT POINTER		
OPTIONS (IF ANY)				PADDING	
ΔΕΔΟΜΕΝΑ (DATA)					
...					

11-1. Εγκατάσταση σύνδεσης TCP



11-2. Τερματισμός σύνδεσης TCP



11-3. Κωδικοποίηση (code bits)

Το πεδίο Code bits περιλαμβάνει 6 Bits τα οόια σηματοδοτούν κάποιες λειτουργίες ή φάσεις της σύνδεσης

bit πεδίου CODE BITS (αριστερά προς τα δεξιά)	Σημασία του bit όταν είναι 1
URG	URGENT POINTER ενεργός (άμεση προώθηση)
ACK	Το bit AKNOWLEDGEMENT είναι ενεργό
PSH	Το τμήμα αυτό να σταλεί άμεσα ανεξάρτητα αν έχει γεμίσει ο buffer (λειτουργία push)
RST	επαναφορά (reset) της σύνδεσης
SYN	Συγχρονισμός αριθμών σειράς πακέτων
FIN	Ο πομπός έχει φτάσει στο τέλος των δεδομένων που έχει να στείλει

12-1. Έλεγχος συμφόρησης στο TCP

- Ο ρυθμός αποστολής του TCP παρακολουθεί τις συνθήκες του δικτύου και μειώνεται (γεωμετρικά) όταν αντιλαμβάνεται συμφόρηση, ενώ αυξάνει (γραμμικά) όταν η ροή εξελίσσεται κανονικά.
- Η κατάσταση στο δίκτυο εικάζεται έμμεσα από την καθυστέρηση των επιβεβαιώσεων (ACK) που υποδηλεί μεγάλες ουρές στους ενδιάμεσους κόμβους, ή πολλαπλά ACK που υποδηλούν απώλειες από υπερχείλιση.
- Ο ρυθμός ελέγχεται μέσω μεταβολών του παραθύρου συμφόρησης (πρβλ με παράθυρο που αποστέλλει ο δέκτης για έλεγχο ροής)

Προβληματισμοί

- Πως μπορεί να γνωρίζει ο πομπός ότι η πληροφορία (τα πακέτα) έφτασε σωστά;
- Με τί ταχύτητα πρέπει να αποστέλλονται τα πακέτα προς το δέκτη;

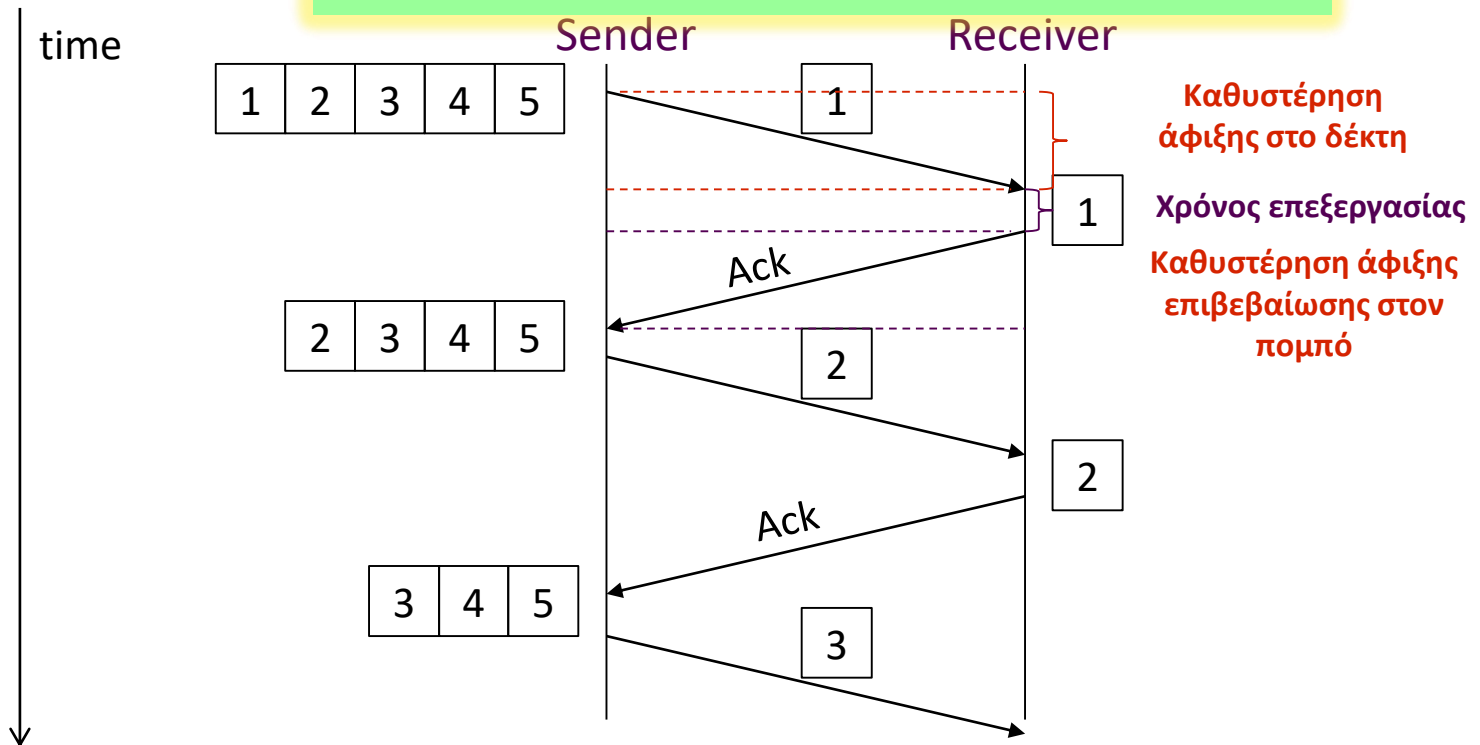


Εξασφάλιση ορθής λήψης

- Πως ξέρει ο αποστολέας ότι ένα πακέτο έφθασε σωστά;

Επιβεβαίωση: μήνυμα από τον παραλήπτη που βεβαιώνει την ορθή λήψη του πακέτου

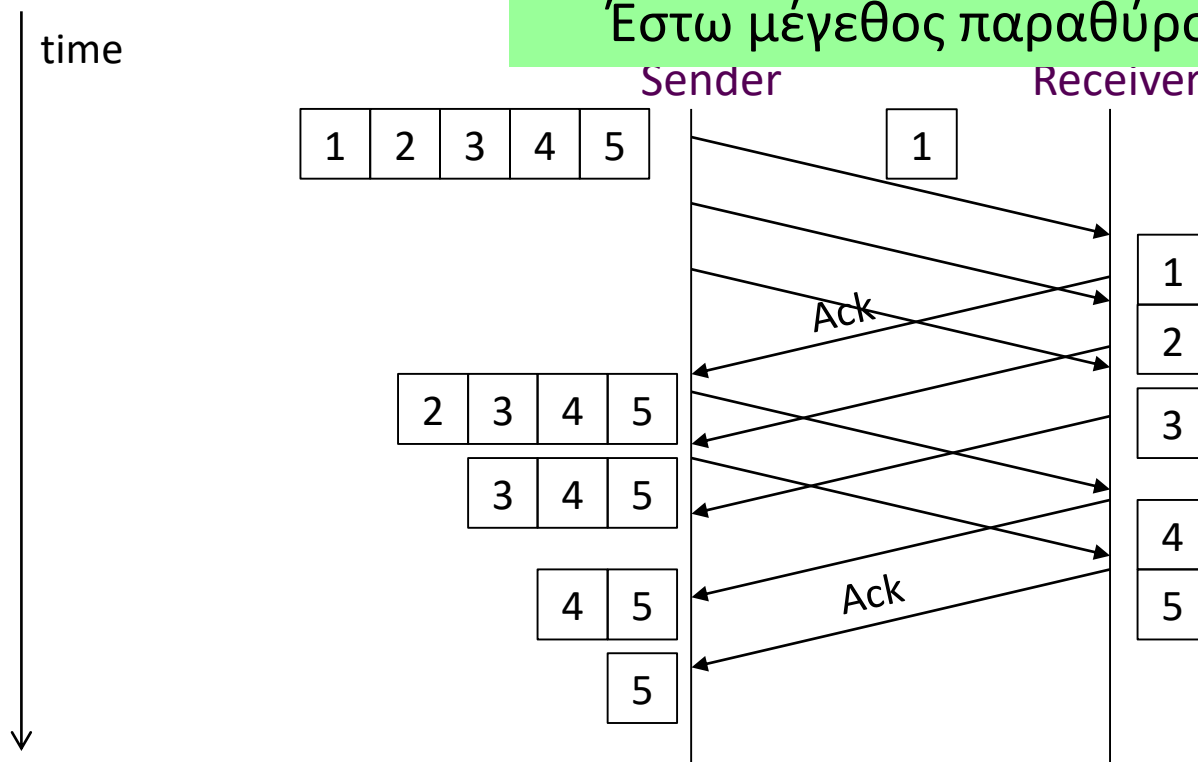
STOP and WAIT



Η έννοια του παραθύρου (I)

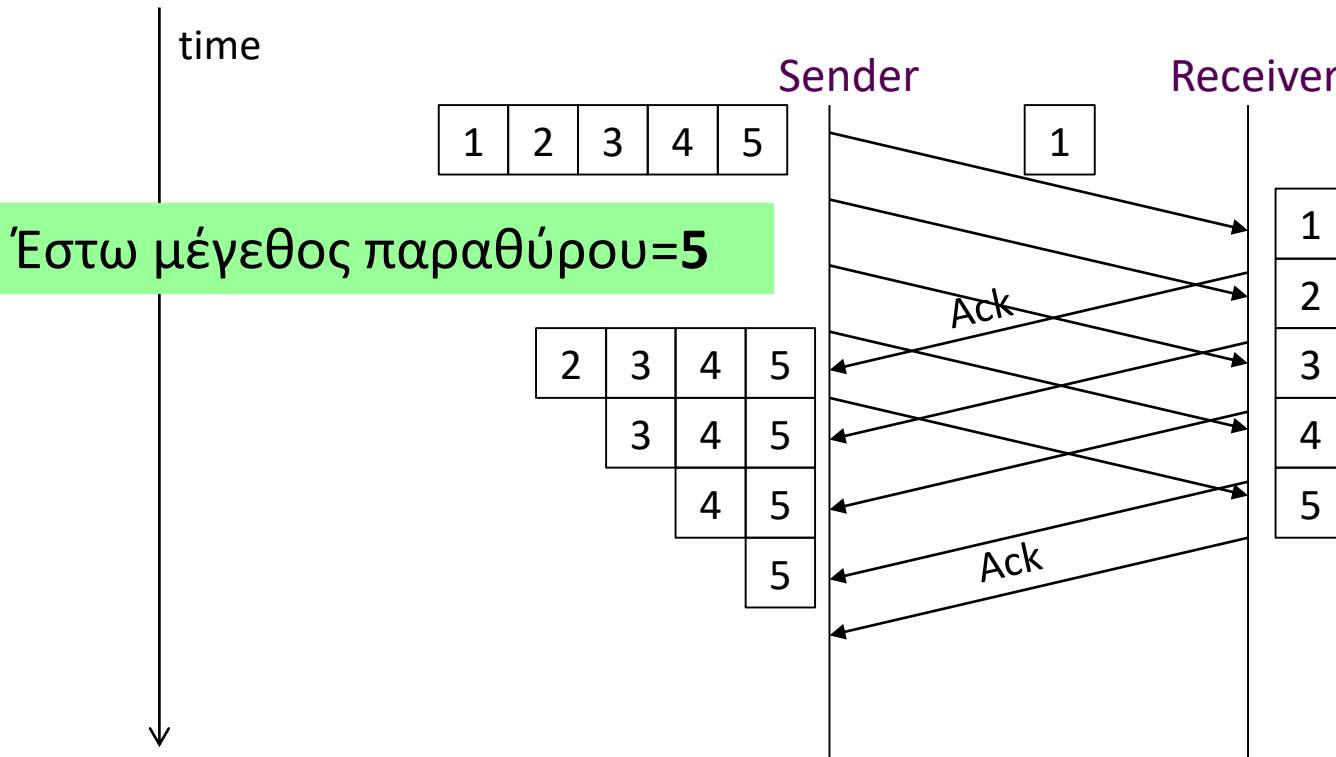
Παράθυρο: τα δεδομένα που επιτρέπεται να βρίσκονται «καθ' οδόν» (μη επιβεβαιωμένα)

Έστω μέγεθος παραθύρου=3



Η έννοια του παραθύρου (II)

Παράθυρο: το δεδομένα που επιτρέπεται να βρίσκονται «καθ' οδόν» (μη επιβεβαιωμένα)



Προβληματισμοί (I)

1. Η χρησιμοποίηση της ζεύξης επηρεάζεται από το μέγεθος του παραθύρου.

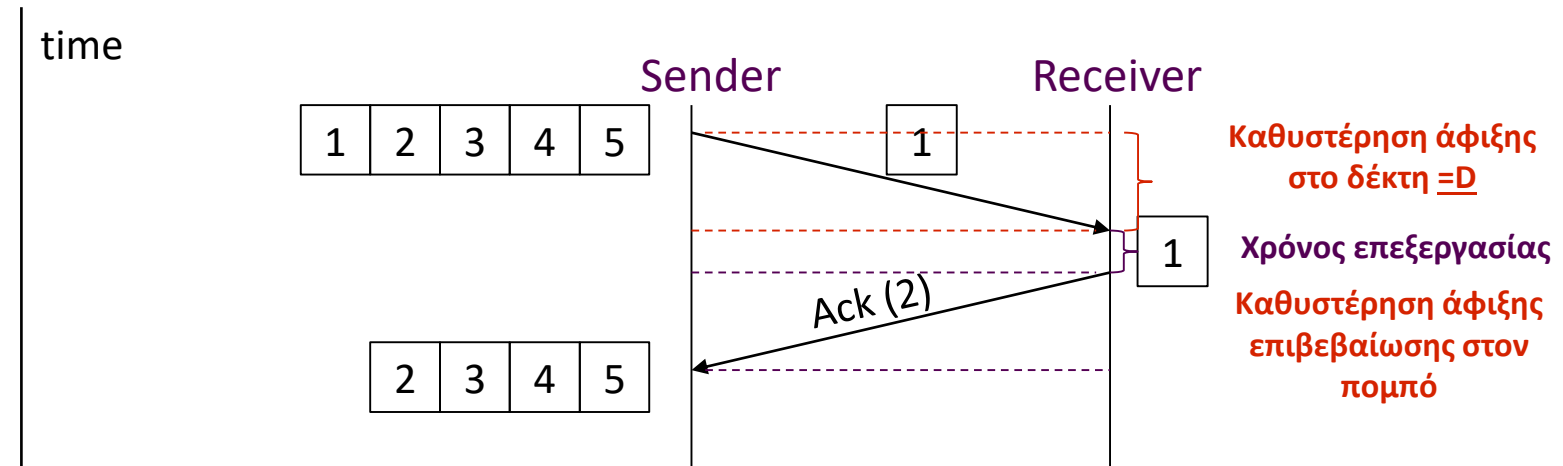
Αλλά ποιο μέγεθος παραθύρου είναι το «σωστό»;

2. Τί συμβαίνει αν χαθεί ένα πακέτο;

Αναμετάδοση, αλλά με ποια πολιτική



Το ιδανικό μέγεθος παραθύρου



Θα πρέπει να υπολογίσουμε πόσα bit «χωράνε» στη ζεύξη
Γινόμενο εύρους ζώνης- καθυστέρησης
(bandwidth –delay product)

Έστω BD το γινόμενο αυτό εκφρασμένο σε αριθμό πλαισίων

$$W = 2 * BD + 1$$

Για να μένει ο πομπός ενεργός καθ'όλη τη διάρκεια του RTT

Γιατί δεν πρόκειται ο δέκτης να στείλει επιβεβαίωση αν δεν λάβει ολόκληρο το πλαίσιο 1

Αξιοποίηση ζεύξης

- 100% αν $w \geq 2BD+1$
- Σε περίπτωση μικρότερου παραθύρου
Αξιοποίηση $\leq w/(2BD+1)$

Προβληματισμοί (II)

1. Η χρησιμοποίηση της ζεύξης επηρεάζεται από το μέγεθος του παραθύρου.

Αλλά ποιο μέγεθος παραθύρου είναι το «σωστό»;

2. Τί συμβαίνει αν χαθεί ένα πακέτο;

Αναμετάδοση αλλά με ποια πολιτική



Πολιτική αναμετάδοσης

- Οπισθοχώρηση κατά n (Go-Back n)
- Επιλεκτική αναμετάδοση (Selective Repeat)
- Ποια είναι η καλύτερη;

Τι είπαμε μέχρι τώρα?

- Γιατί χρειάζονται οι επιβεβαιώσεις;
- Τί εξυπηρετεί ο μηχανισμός παραθύρου;
- Μπορείτε να υπολογίσετε το ιδανικό παράθυρο στο διαδίκτυο;

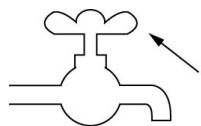
Το παράθυρο στο διαδίκτυο

Το παράθυρο στο διαδίκτυο

- Στόχος
 - η αποφυγή υπερχείλισης στο δέκτη (έλεγχος ροής)
 - η αποφυγή συμφόρησης στο δίκτυο

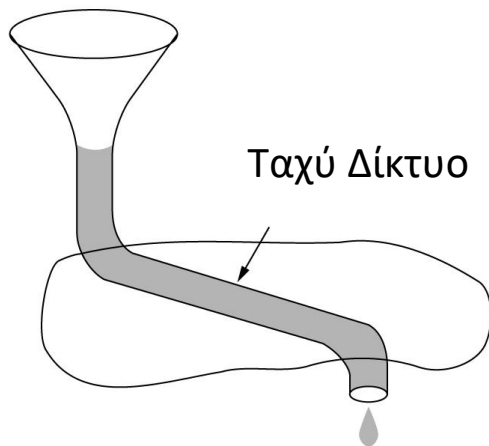
Το πρόβλημα

Πομπός



Ρύθμιση ροής

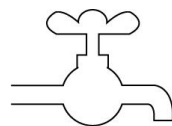
Έλεγχος ροής



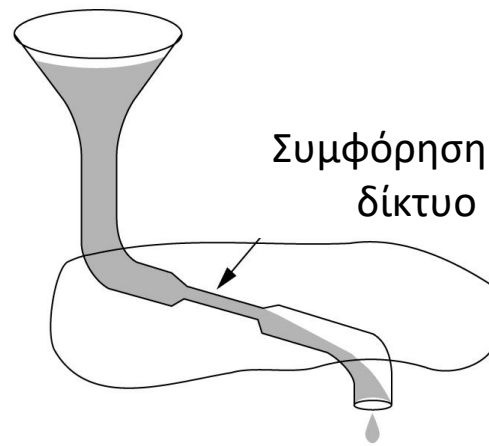
Δέκτης μικρής χωρητικότητας



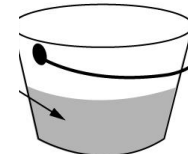
Απώλεια πακέτων στο δέκτη



Αποφυγή συμφόρησης



Δέκτης μεγάλης χωρητικότητας



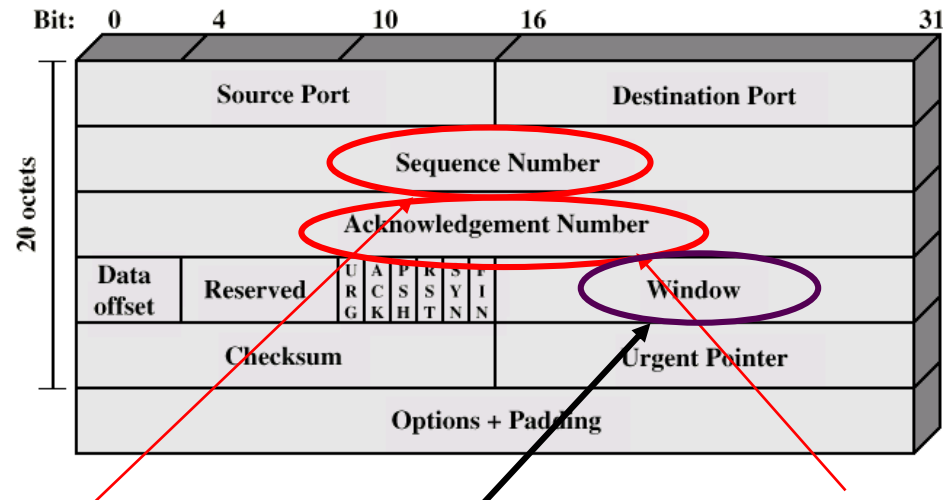
Απώλεια πακέτων στο δίκτυο

TCP: μεταβλητό παράθυρο

- Transmission Control Protocol
- Προσδιορισμός τιμή παραθύρου
 - Ο δέκτης δηλώνει το διαθέσιμο χώρο στη μνήμη του (στα πεδία της επικεφαλίδας του TCP) ίσο με credit
 - Έλεγχος ροής
 - Ο πομπός υπολογίζει την τιμή **congestion window** (cwnd) με βάση την κατάσταση του δικτύου
 - Αποφυγή συμφόρησης
 - Ο πομπός χρησιμοποιεί για τη μετάδοση ως τιμή παραθύρου
$$awnd = \mathbf{MIN}[credit, cwnd]$$

Τα πεδία του TCP

- Κάθε τεμάχιο φέρει στην επικεφαλίδα



Αριθμός ακολουθίας (seq number):

Κατά την αποστολή, αφορά την πρώτη οκτάδα δεδομένων

Αριθμός επιβεβαίωσης

(Ack Number AN=i) επιβεβαιώνει την ορθή λήψη όλων των οκτάδων μέχρι και την i-1.

Μέγεθος παραθύρου (window size $W=j$)

δίνει την άδεια στον πομπό να στείλει j ακόμα οκτάδες

Διαχείριση παραθύρου συμφόρησης (I)

Για το cwnd:

- **Αργή εκκίνηση** (Slow start)
 - Αρχικοποίηση σε τιμή ≤ 2 (χρησιμοποιείται κατά την εκκίνηση)
 - Αύξηση του παραθύρου συμφόρησης κατά ένα με την άφιξη της πρώτης επιβεβαίωσης.
 - Εκθετική αύξηση στη συνέχεια με τη λήψη κάθε επιβεβαίωσης
- Η εκθετική αύξηση τερματίζεται εφόσον ξεπεραστεί μία τιμή κατωφλίου (`ss_threshold`) οπότε το TCP εισέρχεται στη φάση **Congestion Avoidance**

Διαχείριση παραθύρου συμφόρησης (II)

Για το cwnd:

- **Αποφυγή συμφόρησης (Congestion Avoidance)**
 - Όταν $cwnd > ss_threshold$, μείωση του ρυθμού αύξησης από εκθετική σε γραμμική – προσθετική
 - Αύξηση του παραθύρου συμφόρησης κατά ένα κάθε RTT (round-trip-time)

Διαχείριση παραθύρου συμφόρησης (III)

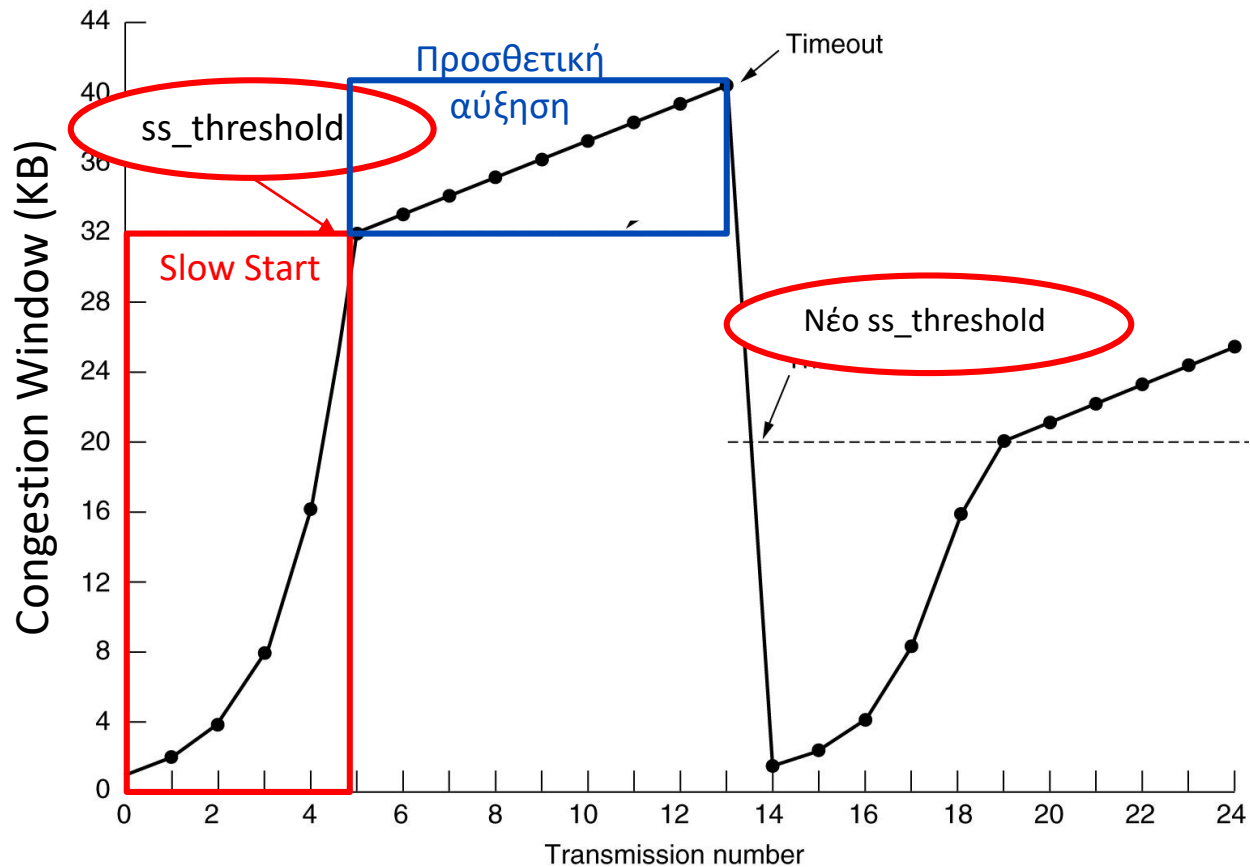
Για το cwnd:

- Η **συμφόρηση** γίνεται αντιληπτή από την απώλεια πακέτου και τότε:
 - Επανάληψη φάσης slow-start
 - Αρχικοποίηση cwnd στο 1
 - Μείωση τιμής κατωφλίου συμφόρησης (ss_threshold) στην τιμή $\frac{1}{2} * cwnd$

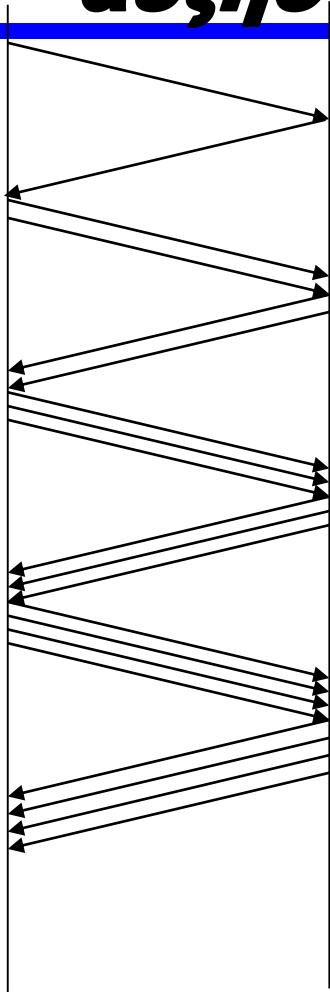
TCP Tahoe

Με πολλαπλές επαναλήψεις αναμένεται η τιμή κατωφλίου συμφόρησης να συγκλίνει περίπου στο $\frac{1}{2}$ του διαθέσιμου εύρους ζώνης

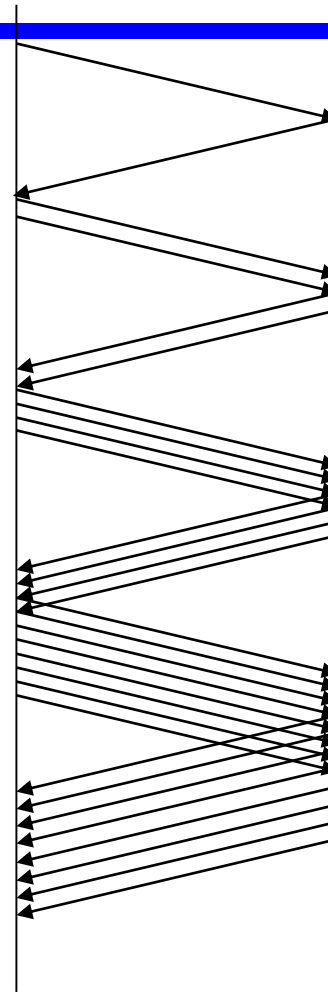
TCP: εξέλιξη παραθύρου συμφόρησης



12-2. Γραμμική-εκθετική αύξηση

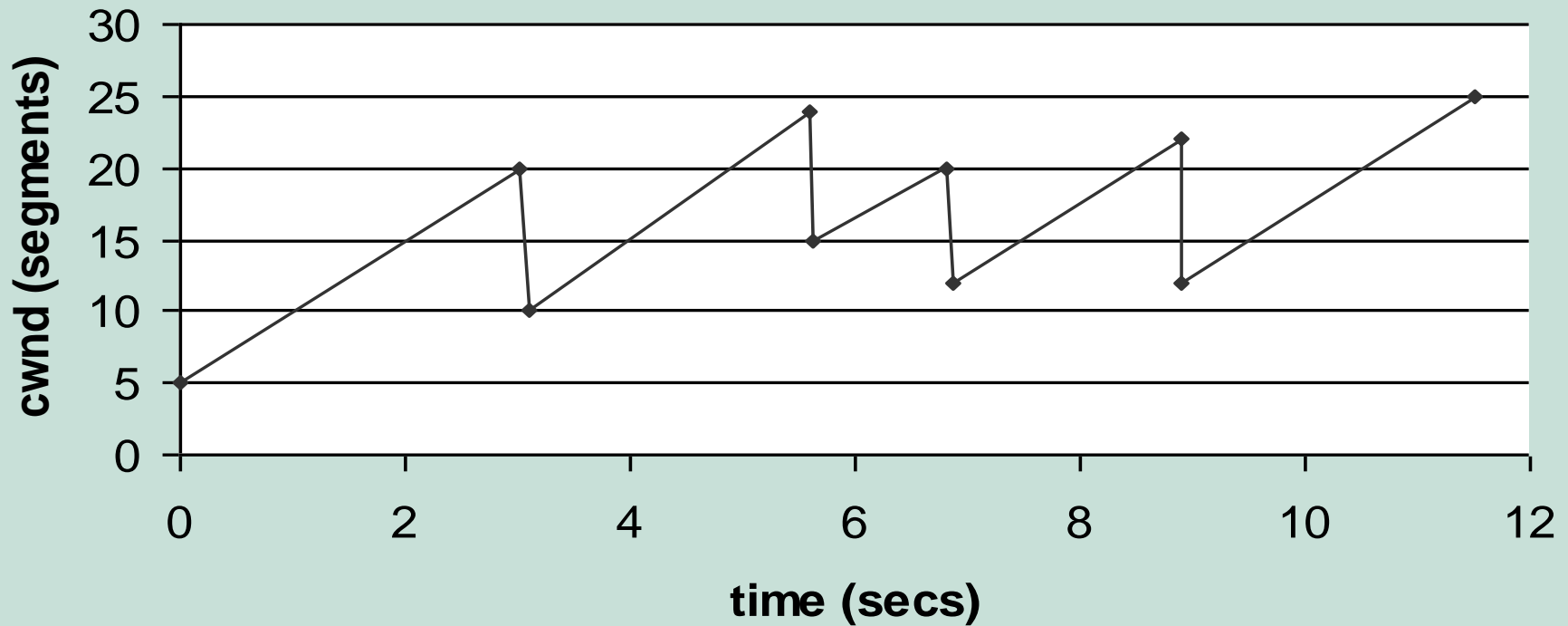


Στο σχήμα αριστερά ο πομπός στέλνει μετά κάθε επιβεβαίωση που δέχεται ένα τμήμα (πακέτο) περισσότερο κάθε φορά και έτσι ο ρυθμός αποστολής αυξάνει γραμμικά

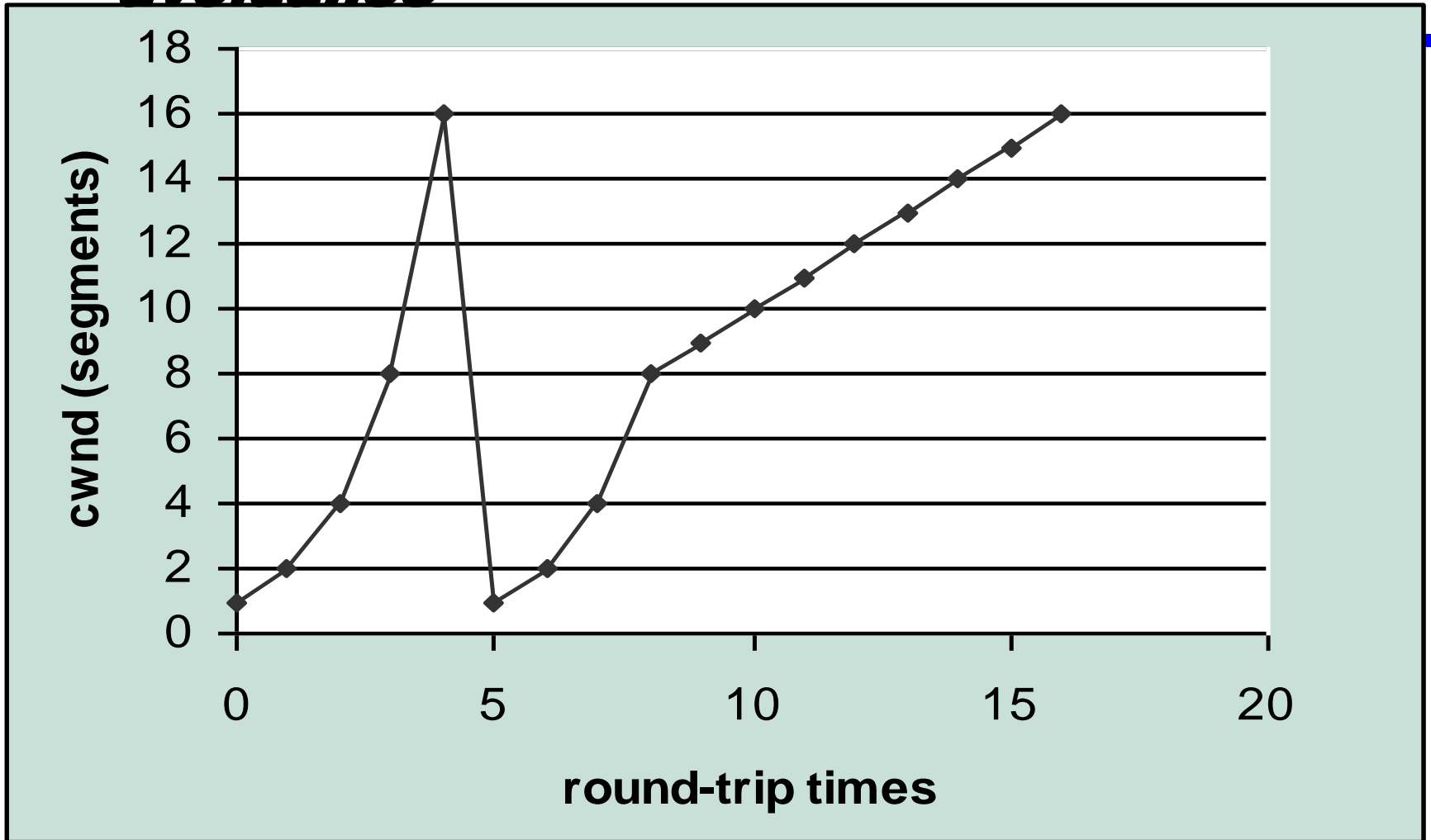


Στο σχήμα δεξιά με κάθε επιβεβαίωση ο πομπός στέλνει διπλάσια τμήματα (πακέτα) κάθε φορά και έτσι ο ρυθμός αποστολής αυξάνει γεωμετρικά (εκθετικά)

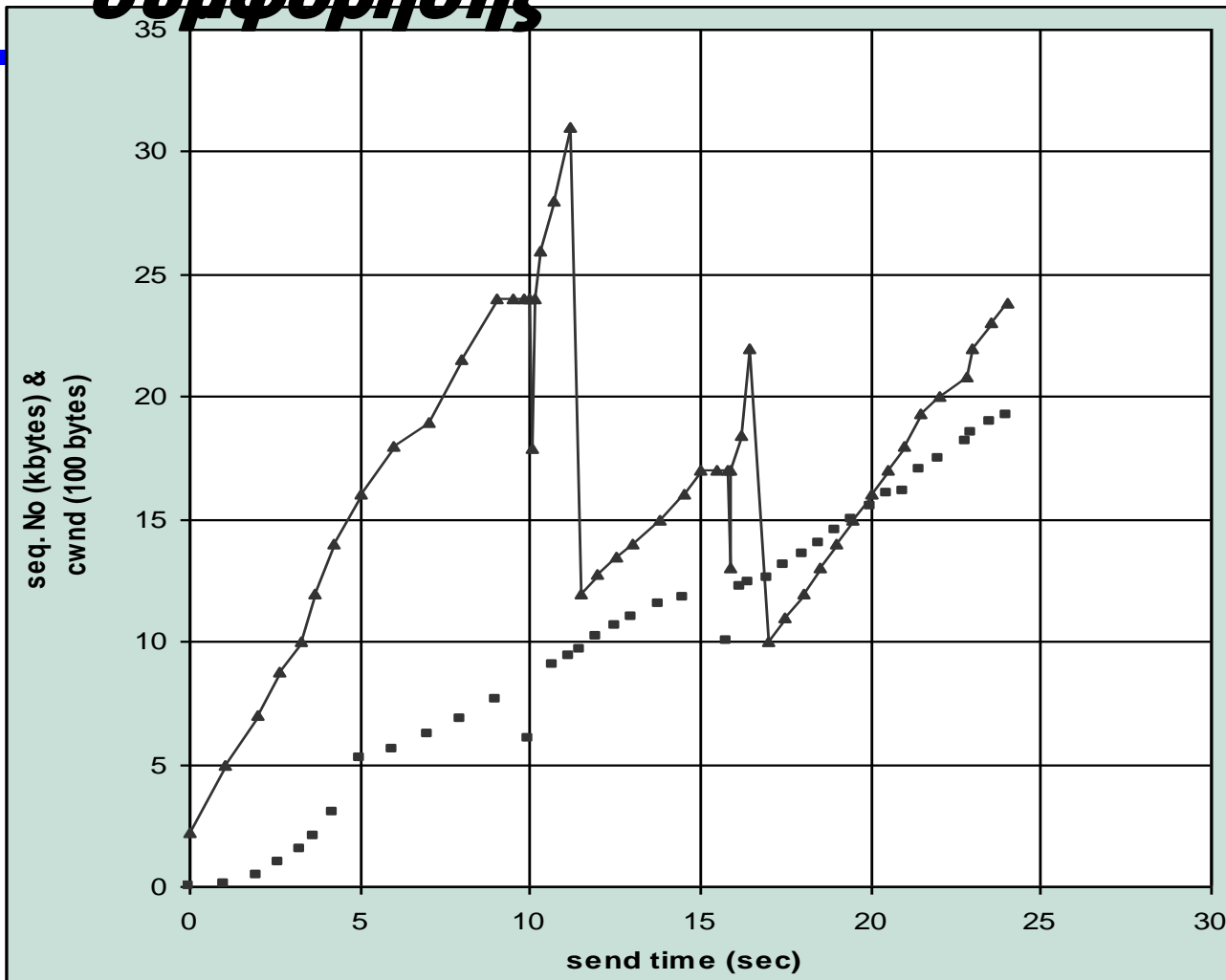
12-3. Εξέλιξη παραθύρου συμφόρησης



12-4. Slow start & congestion avoidance



12-4. Παράδειγμα ελέγχου συμφόρησης



Στο σχήμα αριστερά με τρίγωνα συνδεδεμένα με γραμμές φαίνεται η εξέλιξη του παραθύρου συμφόρησης. Ενώ με τετραγωνάκια η εξέλιξη των αριθμών σειράς των πακέτων. Διακρίνονται οι αναμεταδόσεις στα 10 sec και 16 sec

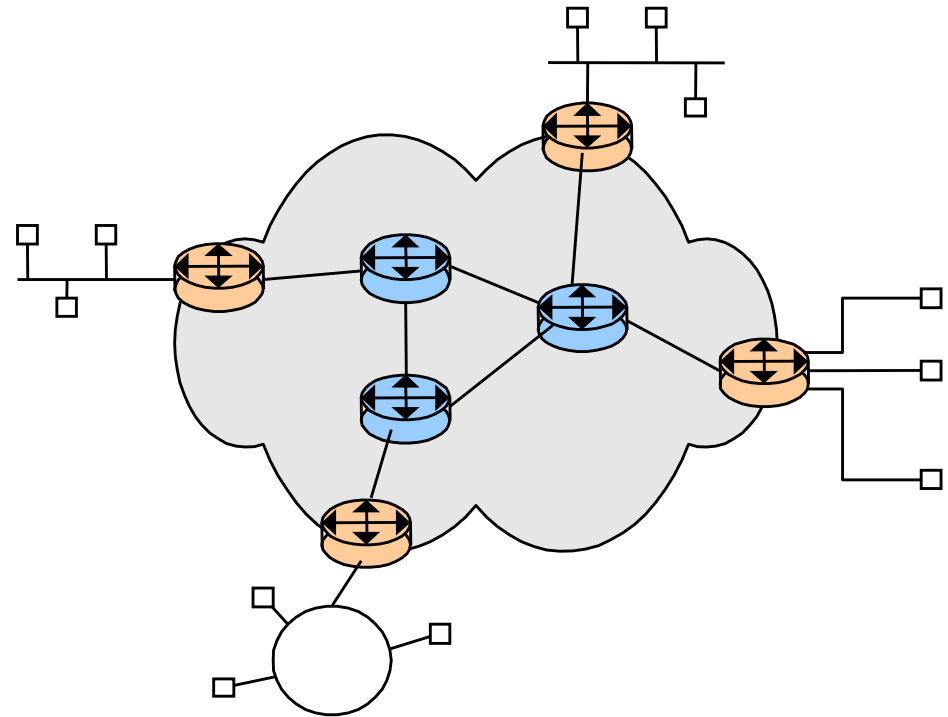
ΜΕΤΑΓΩΓΗ ΕΤΙΚΕΤΤΑΣ

ΠΟΛΛΑΠΛΩΝ ΠΡΩΤΟΚΟΛΛΩΝ

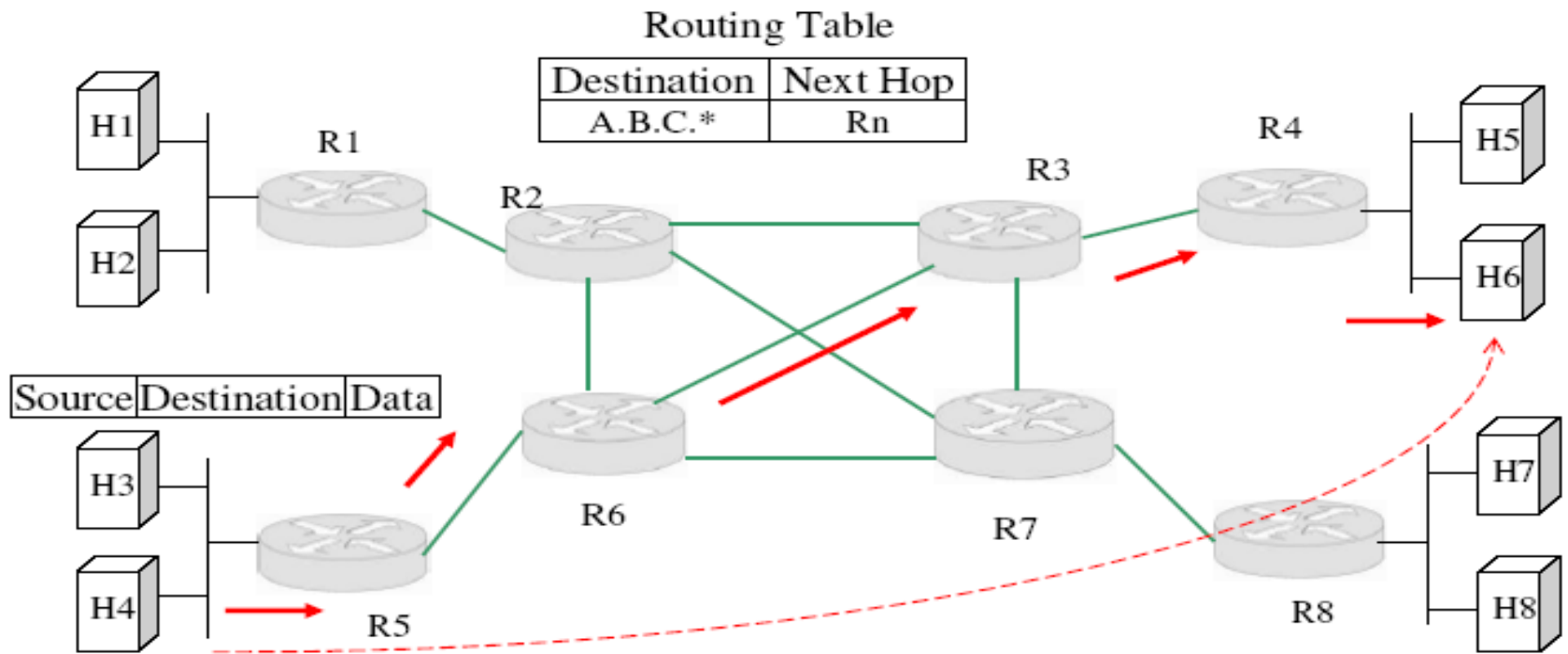
Multi-Protocol Label Switching

Συμβατικά Δίκτυα IP

- Δρομολογητές
 - Ακραίοι (Απόληξης)
 - Ενδιάμεσοι (Πυρήνα)
- Δρομολόγηση
 - Hop-by-hop
 - Εξετάζει επικεφαλίδα επιπέδου 3 (IP)
- Υπηρεσία χωρίς σύνδεση
- Σύγκριση με μοντέλο ATM



Δρομολόγηση σε δίκτυο IP



Δρομολογητής IP

Ένας δρομολογητής IP αποτελείται από τα εξής δομικά στοιχεία:

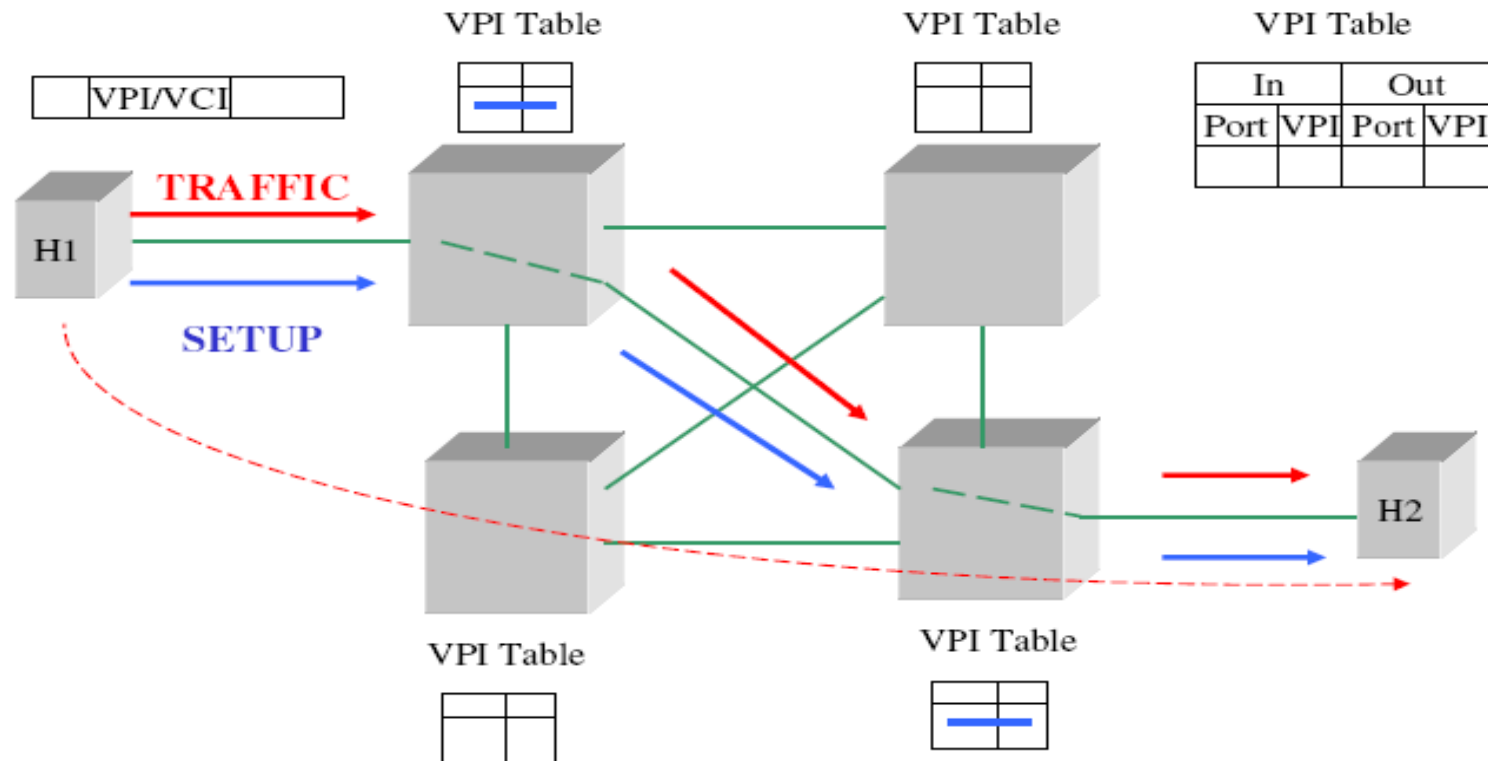
— **στοιχείο ελέγχου (control component)**

- *Χρησιμοποιώντας πρωτόκολλα δρομολόγησης όπως OSPF, BGP, συλλέγονται πληροφορίες για διαδρομές και δρομολόγηση μεταξύ των κόμβων*
- *Το αποτέλεσμα είναι η δημιουργία του πίνακα δρομολόγησης (forwarding information base)*

— **στοιχείο προώθησης (forwarding component)**

- *Υλοποιεί τη λειτουργία της προώθησης πακέτων*
- *Με βάση τη διεύθυνση προορισμού IP αναζητά στην FIB, (χρησιμοποιώντας τον αλγόριθμο longest match) τη διεπαφή εξόδου και τον επόμενο κόμβο*

ATM



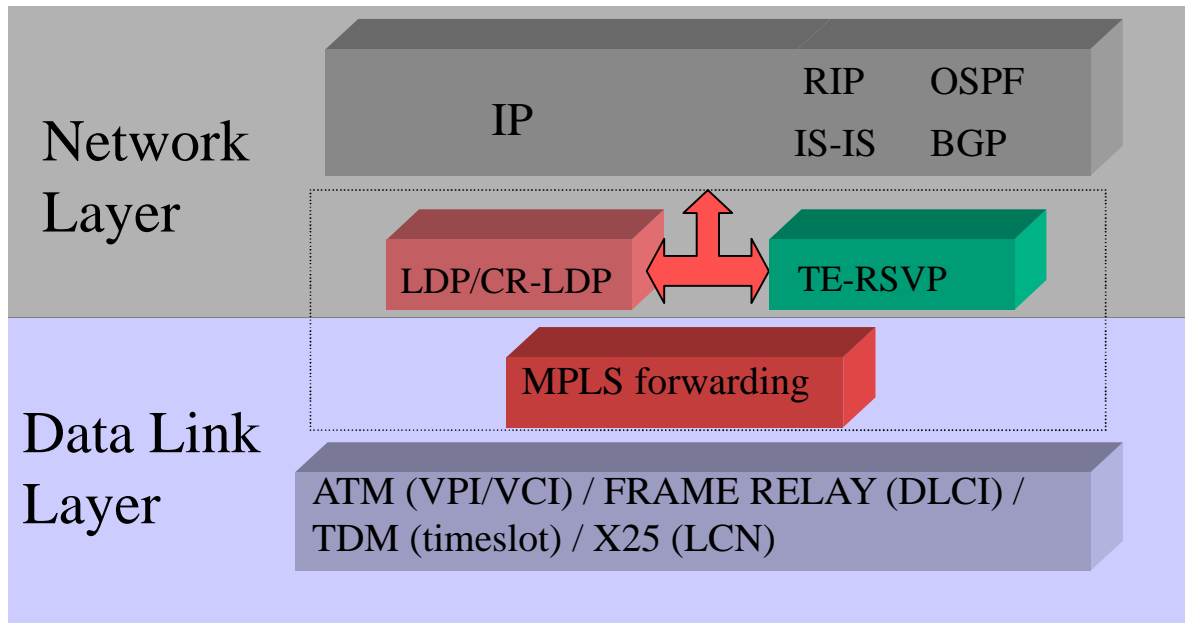
Multi-Protocol Label Switching

Μεταγωγή Ετικέτας Πολλαπλών Πρωτόκολλων

- **Μεταγωγή** αντί για δρομολόγηση
 - Υποδομή δικτύου προσανατολισμένου στη σύνδεση
- Κάνει χρήση **Ετικέτας** για την προώθηση των πακέτων
 - Είναι τεχνολογία προώθησης πακέτων που κάνει χρήση ετικετών (labels) για να αποφασίσει που θα προωθήσει τα εισερχόμενα πακέτα
- **Πολλαπλών Πρωτόκολλων**
 - Εφαρμόζεται μεταξύ επιπέδων 2 & 3 (data link & network)
 - Είναι ανεξάρτητη από πρωτόκολλα του επιπέδου 2 ή 3

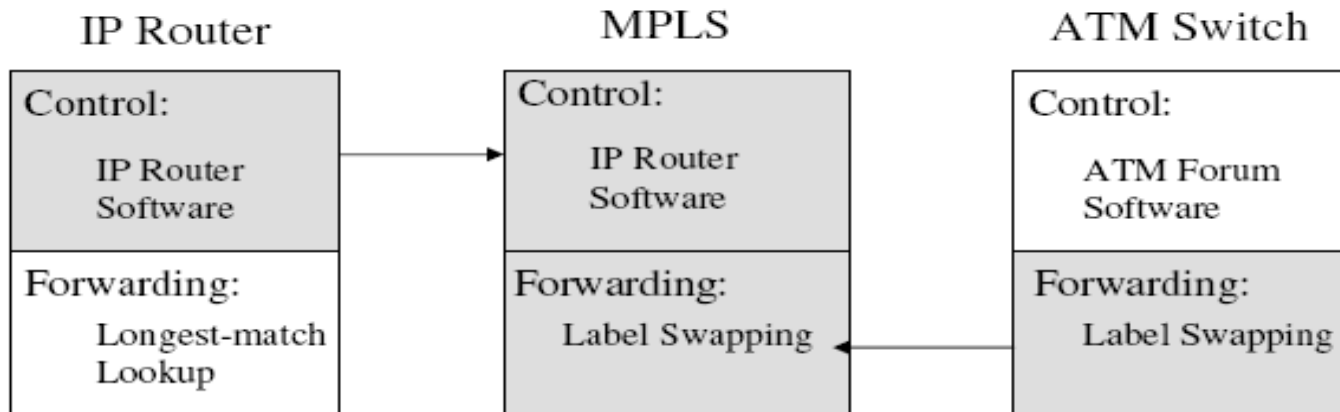
MPLS Forwarding & Control (I)

- Το MPLS χωρίζεται λογικά και λειτουργικά σε δύο κομμάτια ώστε να παρέχει την λειτουργικότητα της μεταγωγής ετικέτας σε ένα δίκτυο χωρίς σύνδεση.



Η διαστρωμάτωση στο MPLS

MPLS Forwarding & Control (II)

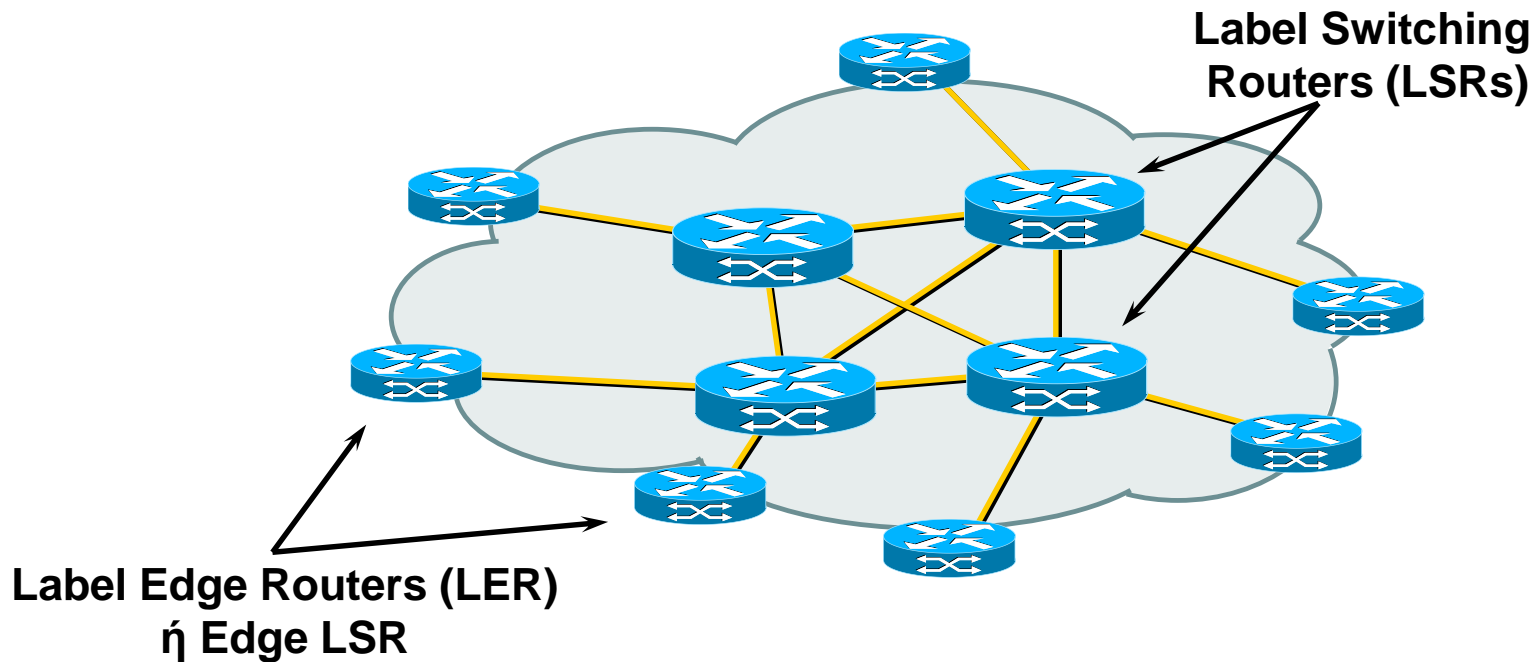


Βασική Ιδέα Προώθησης Πακέτων

- Λειτουργία προώθησης πακέτων στο IP
 - γίνεται ανά πακέτο
 - απαιτητική ως προς υπολογιστική ισχύ
 - Για το λόγο αυτό η τεχνολογία MPLS απλουστεύει την προώθηση πακέτων
- Βασική ιδέα:
 - Οι δρομολογητές απόληξης εκτελούν κανονικά λειτουργία δρομολόγησης
 - Οι δρομολογητές πυρήνα εκτελούν λειτουργία μεταγωγής, η οποία ως λειτουργία επιπέδου 2 είναι πιο γρήγορη

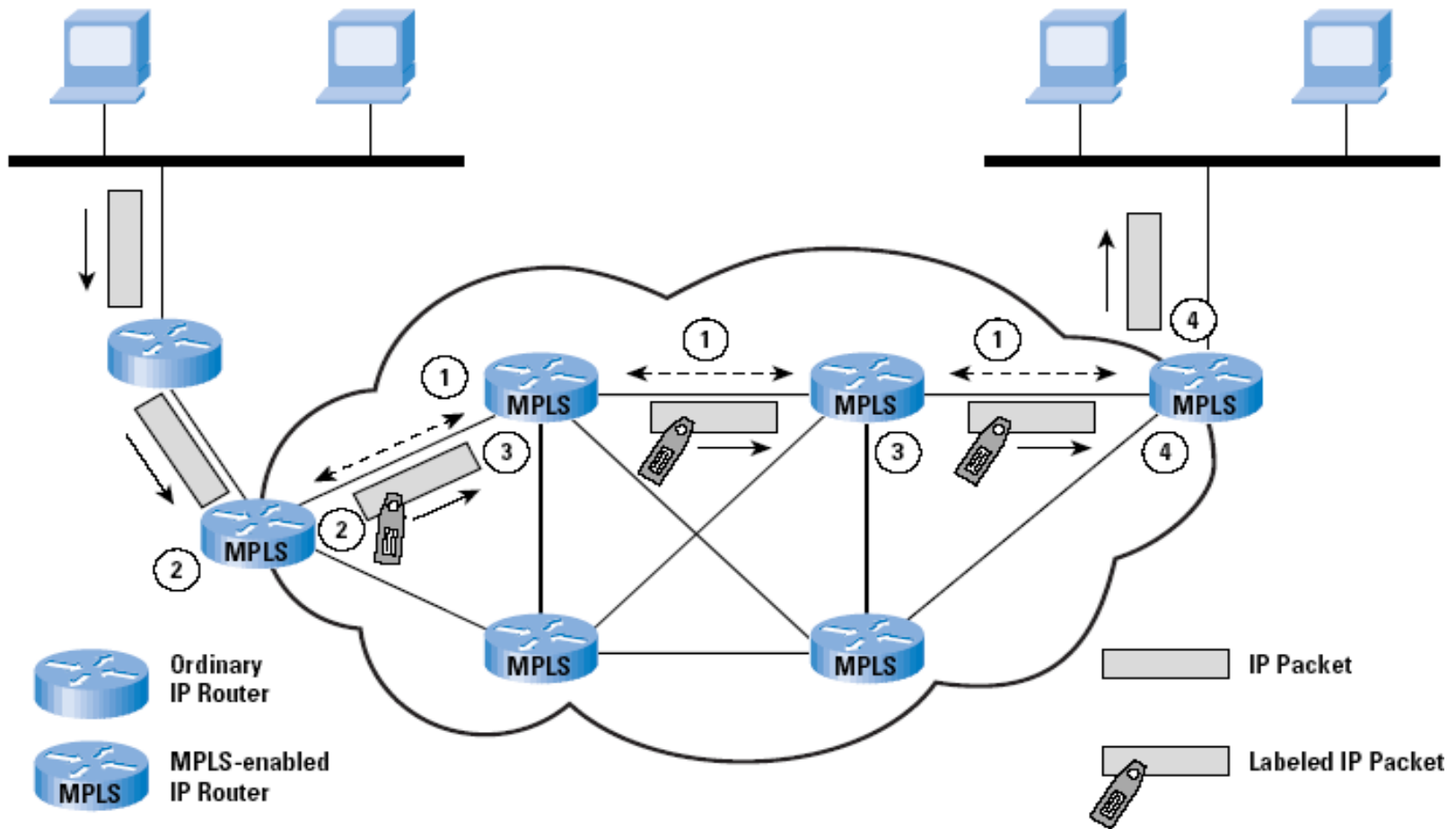
Label Switching Routers

- Οι δρομολογητές του δικτύου πυρήνα αναβαθμίζονται και γίνονται Δρομολογητές-Μεταγωγείς (Label-Switching Routers, LSRs).



Αρχιτεκτονική δικτύου μεταγωγής με ετικέτα

Παράδειγμα Προώθησης Πακέτων

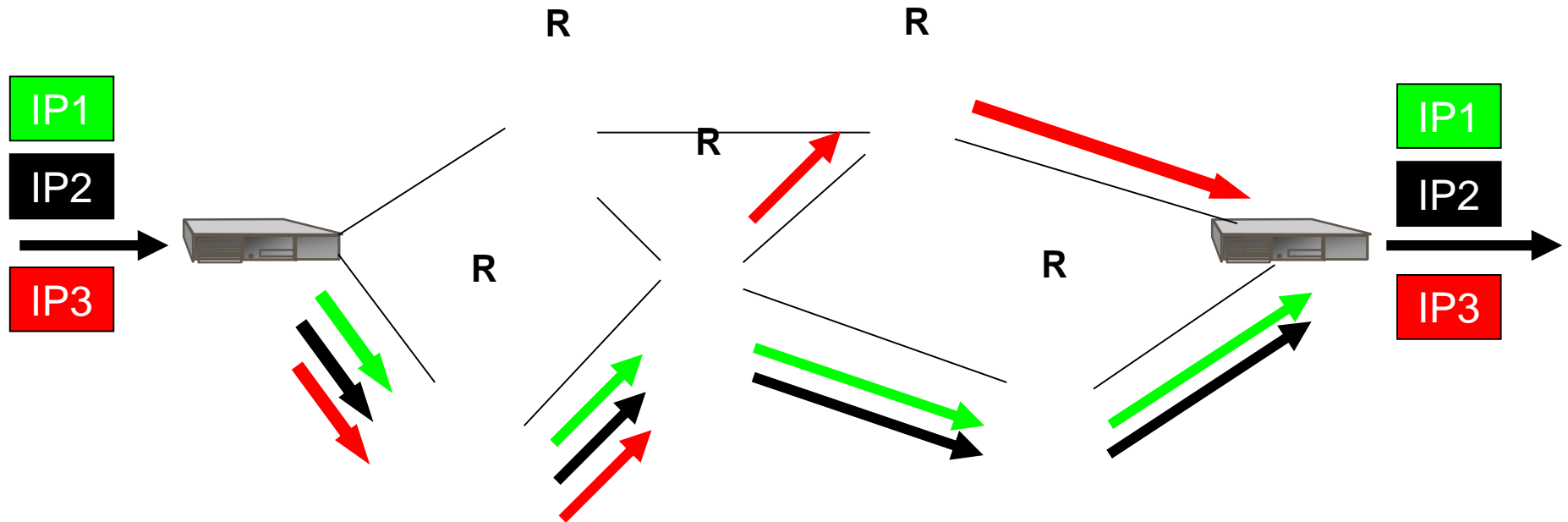


Βασικές Έννοιες MPLS

- Label Switching Router: Δρομολογητής μεταγωγής ετικέτας
- Forwarding Equivalence Class (FEC): Κλάση προώθησης
 - Ροή πακέτων που προωθούνται με τον ίδιο τρόπο
- Label: ετικέτα
- Label Switched Path
 - Η νοητή σύνδεση (μονοπάτι) που ορίζεται από την μεταβολή στις τιμές της ετικέτας
 - Το μονοπάτι καθορίζεται από την αρχική τιμή της ετικέτας
- Label Swap Operation
 - Η διαδικασία αλλαγής της ετικέτας στους ενδιάμεσους LSRs
- Label Information Base (LIB)
 - Πίνακας προώθησης πακέτων με βάση την ετικέτα σε κάθε LSR
- Label Distribution Protocol (LDP)
 - Πρωτόκολλο Κατανομής Ετικέτας (ενημέρωση των LIB)

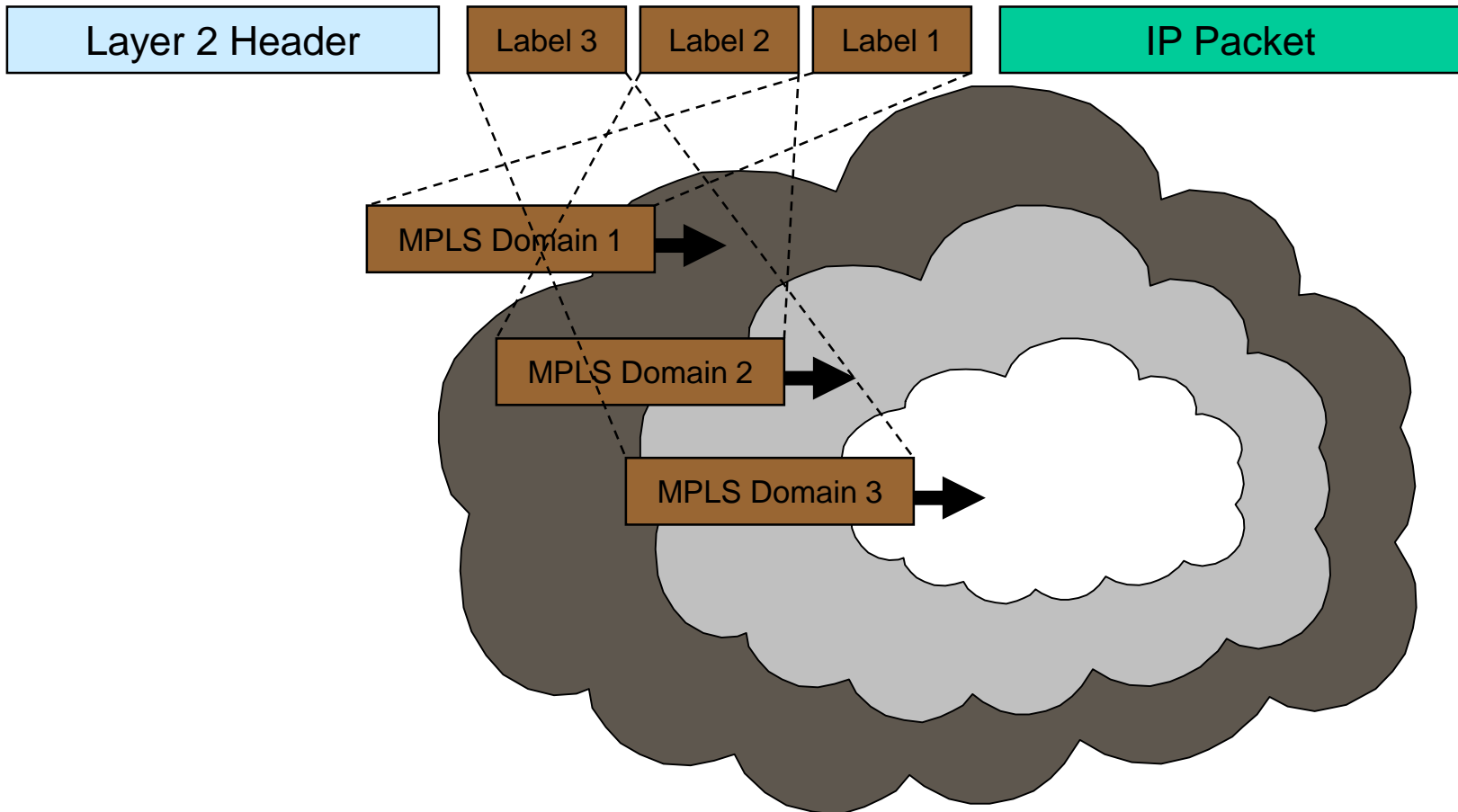
Forwarding Equivalence Class (FEC)

- Το σύνολο των IP πακέτων που προωθούνται με τον ίδιο τρόπο (π.χ. Από το ίδιο μονοπάτι, με την ίδια αντιμετώπιση)



Γενικά, η κλάση συσχετίζεται με συγκεκριμένη συμπεριφορά του δικτύου. Στο παραπάνω παράδειγμα, λαμβάνοντας μόνο υπόψιν το μονοπάτι, τα πακέτα 1 και 2 ανήκουν στην ίδια κλάση, ενώ το 3 όχι.

Label Stack – στοίβα ετικετών



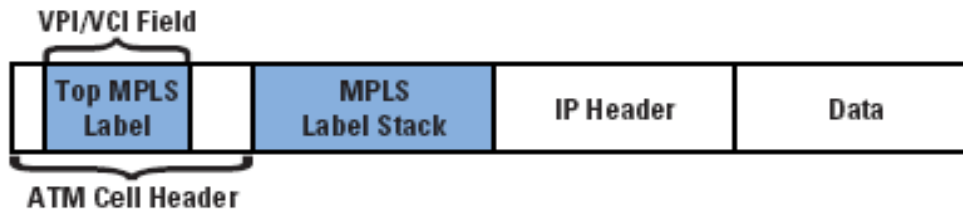
Η θέση της ετικέτας στο πακέτο



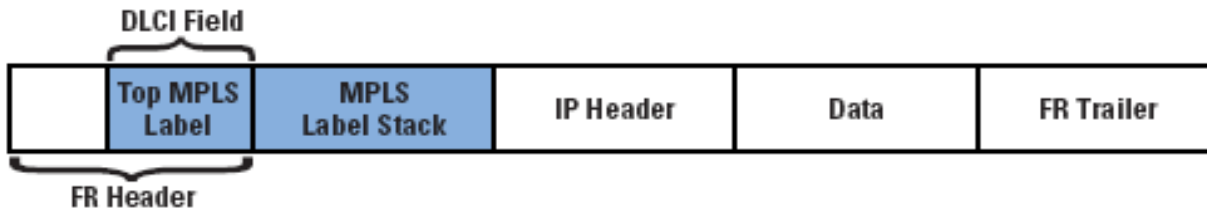
(a) Data Link Frame



(b) IEEE 802 MAC Frame



(c) ATM Cell



(d) Frame Relay Frame

LDP Πρωτόκολλο Κατανομής Ετικέτας (ενημέρωση των LIB)

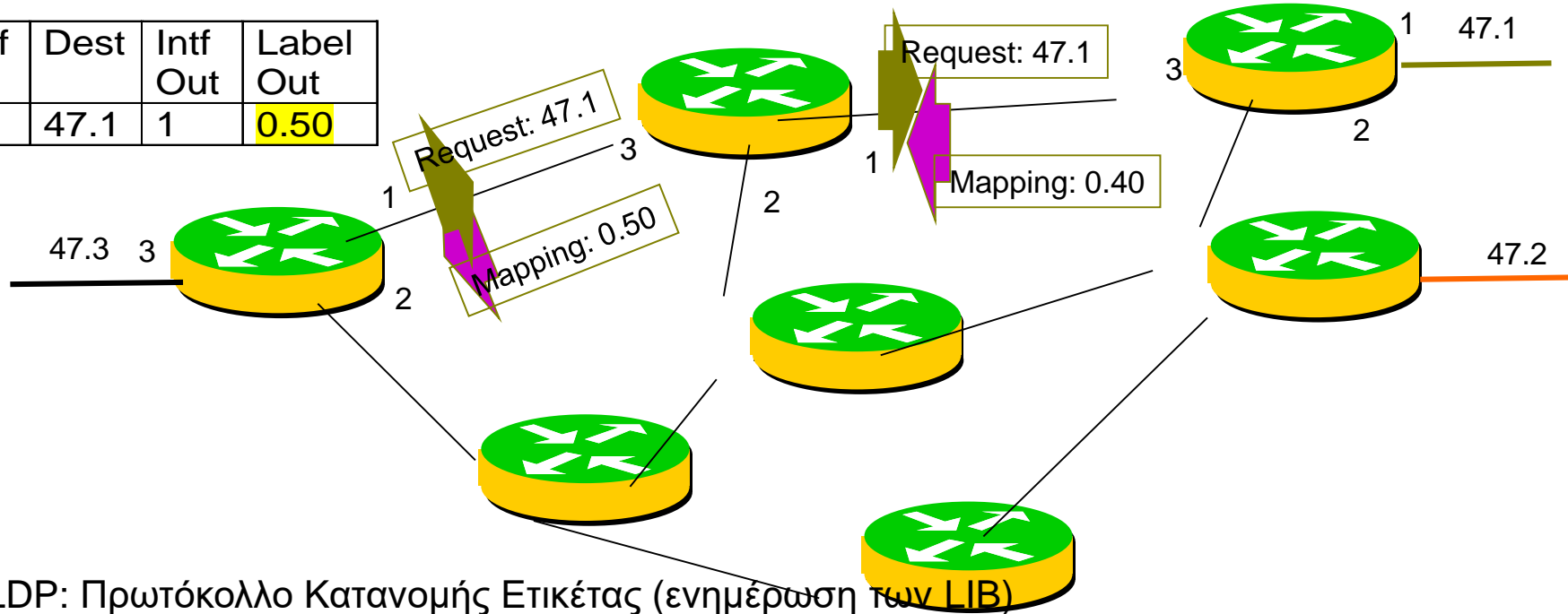
LIB: βάση πληροφοριών ετικέτας

MPLS Label Distribution based on routing table

Intf In	Label In	Dest	Intf Out	Label Out
3	0.50	47.1	1	0.40

Intf In	Label In	Dest	Intf Out
3	0.40	47.1	1

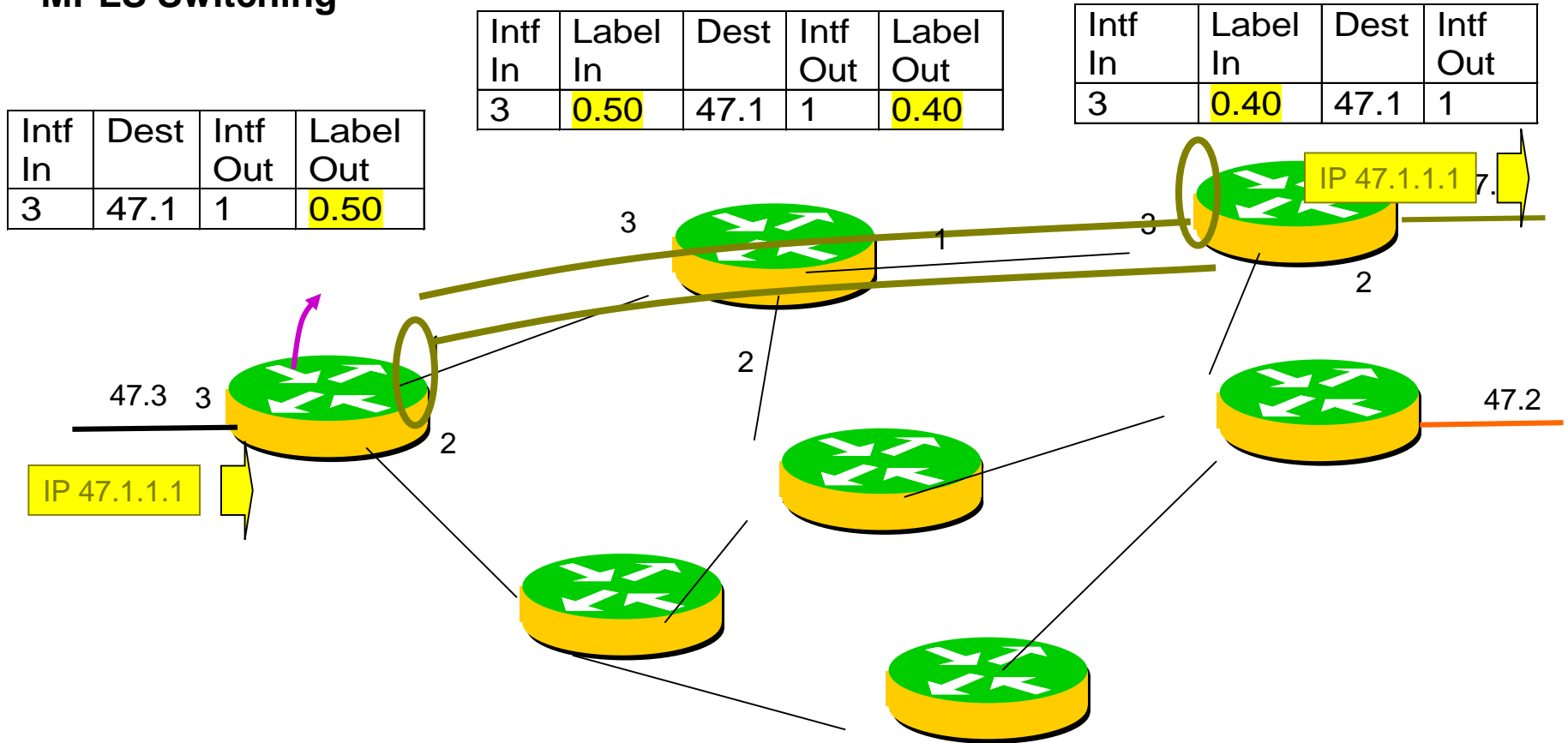
Intf In	Dest	Intf Out	Label Out
3	47.1	1	0.50



LDP: Πρωτόκολλο Κατανομής Ετικέτας (ενημέρωση των LIB)

LSP

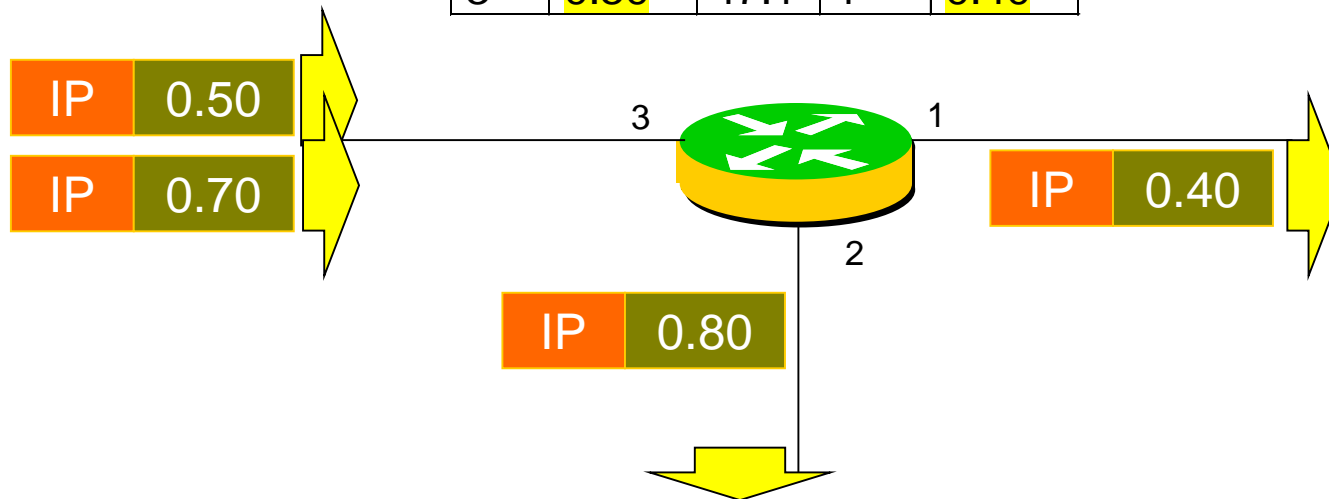
MPLS Switching



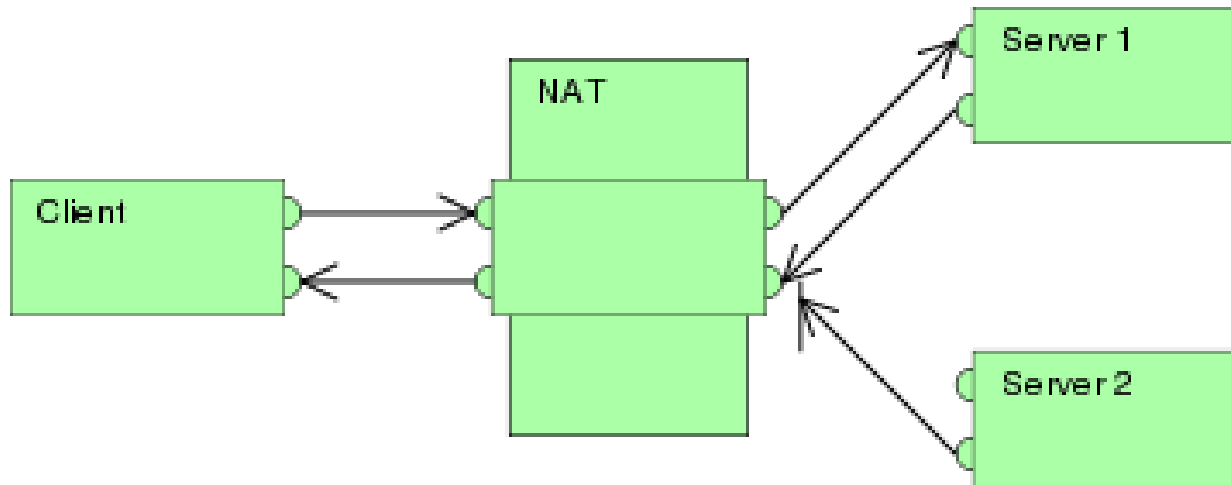
LSP: μονοπάτι που ορίζεται από την μεταβολή στις τιμές της ετικέτας

Label Swap – Αντιμετάθεση ΕΤΙΚΕΤΑΣ

Intf In	Label In	Dest	Intf Out	Label Out
3	0.70	47.2	2	0.80
3	0.50	47.1	1	0.40



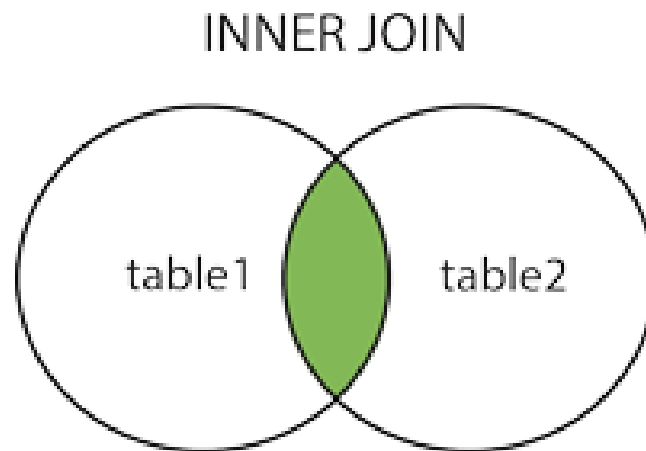
Network Address Translation Protocol



-
- Συμπληρωματικά παραδείγματα SQL

Παραδείγματα Inner Join (I)

- `SELECT Orders.OrderID, Customers.CustomerName
FROM Orders
INNER JOIN Customers ON Orders.CustomerID =
Customers.CustomerID;`



- Το αποτέλεσμα είναι πίνακας με τόσες γραμμές όσες και τα κοινά στοιχεία

Παραδείγματα Inner Join (II)

- `SELECT Orders.OrderID, Customers.CustomerName
FROM Orders
INNER JOIN Customers ON Orders.CustomerID =
Customers.CustomerID;`

OrderID	CustomerID	EmployeeID	OrderDate	ShipperID
10308	2	7	1996-09-18	3
10309	37	3	1996-09-19	1
10310	77	8	1996-09-20	2

and a selection from the "Customers" table:

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitución 2222	México D.F.	05021	Mexico
3	Antonio Moreno Taqueria	Antonio Moreno	Mataderos 2312	México D.F.	05023	Mexico

Παράδειγμα (II)

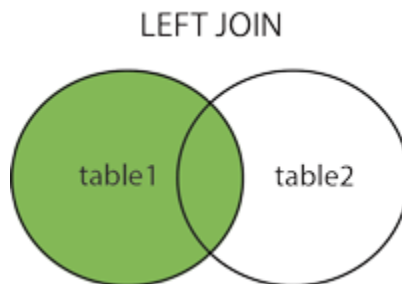
```
SELECT Orders.OrderID,  
Customers.CustomerName, Shippers.ShipperName  
FROM ((Orders  
INNER JOIN Customers ON Orders.CustomerID =  
Customers.CustomerID)  
INNER JOIN Shippers ON Orders.ShipperID =  
Shippers.ShipperID);
```

Number of Records: 3

ShipperID	ShipperName	Phone
1	Speedy Express	(503) 555-9831
2	United Package	(503) 555-3199
3	Federal Shipping	(503) 555-9931

LEFT JOIN

- The LEFT JOIN keyword returns all records from the left table (table1), and the matched records from the right table (table2). The result is NULL from the right side, if there is no match.
- ```
SELECT column_name(s)
FROM table1
LEFT JOIN table2 ON table1.column_name = table2.column_name;
```



# Παράδειγμα LEFT JOIN (I)

---

- ```
SELECT Customers.CustomerName, Orders.OrderID  
FROM Customers  
LEFT JOIN Orders ON Customers.CustomerID =  
Orders.CustomerID  
ORDER BY Customers.CustomerName;
```
- Το αποτέλεσμα έχει τόσες γραμμές όσες οι customers*orders per customer

UNION (I)

The UNION operator is used to combine the result-set of two or more SELECT statements.

- Each SELECT statement within UNION must have the same number of columns
- The columns must also have similar data types
- The columns in each SELECT statement must also be in the same order
- ```
SELECT column_name(s) FROM table1
UNION
SELECT column_name(s) FROM table2;
```

# Παράδειγμα UNION (I)

```
SELECT City FROM Customers
UNION
SELECT City FROM Suppliers
ORDER BY City;
```

| CustomerID | CustomerName                       | ContactName    | Address                       | City        | PostalCode | Country |
|------------|------------------------------------|----------------|-------------------------------|-------------|------------|---------|
| 1          | Alfreds Futterkiste                | Maria Anders   | Obere Str. 57                 | Berlin      | 12209      | Germany |
| 2          | Ana Trujillo Emparedados y helados | Ana Trujillo   | Avda. de la Constitución 2222 | México D.F. | 05021      | Mexico  |
| 3          | Antonio Moreno Taquería            | Antonio Moreno | Mataderos 2312                | México D.F. | 05023      | Mexico  |

And a selection from the "Suppliers" table:

| SupplierID | SupplierName               | ContactName      | Address        | City        | PostalCode | Country |
|------------|----------------------------|------------------|----------------|-------------|------------|---------|
| 1          | Exotic Liquid              | Charlotte Cooper | 49 Gilbert St. | London      | EC1 4SD    | UK      |
| 2          | New Orleans Cajun Delights | Shelley Burke    | P.O. Box 78934 | New Orleans | 70117      | USA     |
| 3          | Grandma Kelly's Homestead  | Regina Murphy    | 707 Oxford Rd. | Ann Arbor   | 48104      | USA     |